State Data Privacy Law Tracker

A concise update on the status and content of state consumer data privacy protection laws — both proposed and enacted — compiled by the attorneys of Fox Rothschild's Privacy & Data Security Practice Group.

Fox Rothschild LLP
ATTORNEYS AT LAW

Compiled by Fox Rothschild Associates:
Anahita Anvari, Philadelphia and Ryan Musser, Dallas.

Following California's Lead: State Consumer Data Privacy Protection Laws

Enacted in 2018, the California Consumer Privacy Act (CCPA) took effect in January 2020, posing a host of new data privacy compliance challenges for companies with customers in California or clients who do business in the state, which is the sixth-largest economy in the world.

The law — which has quickly become a model for others states' privacy legislation — affects for-profit companies that collect and process California residents' personal information, have business in the state and meet one of the following three criteria:

- Generate annual gross revenue > $25 million
- Receive or share data of > 50,000 California residents annually
- Derive at least 50% of annual revenue by selling California residents' personal information

Companies that fall under the act must also ensure that any service providers that handle data on their behalf do it in a manner that complies with the law.

CCPA includes a broad definition of personal information and conveys new rights designed to give consumers more control over their data. These include the ability to opt out of having their data sold, to request information on the types of data companies collect and/or a copy of the actual data collected and, in many cases, the right to request that their data be erased.

The law includes per capita fines of up to $2,500 per incident for violations and up to $7,500 per incident for willful violations, and includes a limited private right of action that allows consumers to file lawsuits over data breaches under certain circumstances.

Following the passage of CCPA, a growing number of other states have proposed, and in some cases adopted, similar new laws. However, each is unique and contains provisions that depart from the CCPA in important ways. In addition, California has adopted detailed CCPA regulations to implement its law.

This handy guide summarizes key components of state data privacy laws that have been proposed and enacted across the United States, presenting the information in an easy-to-read chart format, as well as providing an update on the status of pending legislation as of **May 1, 2021.**

Fox Rothschild Privacy & Data Security

Data Privacy Compliance

HIPAA, GDPR, CCPA. Data privacy compliance has become an alphabet soup of federal, state and international acronyms. Fox Rothschild has the knowledge and experience to help clients avoid costly fines and comply with the myriad regulations that govern the data they collect. We help companies comply with state privacy, data security and data reporting laws as well as international privacy and security requirements.

HIPAA Compliance

Fox understands that compliance with the Health Insurance Portability and Accountability Act (HIPAA) isn't limited to hospitals and medical practices. We provide comprehensive services focused on the proper handling of Protected Health Information (PHI) that include:

- Preparing required policies and procedures for health care providers, health plans and business associates
- Drafting business associate agreements, data use agreements for health information exchanges accessed by multiple providers, HIPAA-compliant authorizations for disclosure of PHI and access request forms to be used by covered entities for patient or plan member PHI access requests
- Providing HIPAA compliance reviews for researchers receiving or using PHI
- Reviewing mergers/acquisitions of HIPAA-covered entities and business associates: due diligence and handling PHI; representations and warranties related to HIPAA compliance and breaches discovered after closing
- Providing breach and security incident response and analysis.
- Responding to Office of Civil Rights (OCR) investigations.

GDPR Compliance

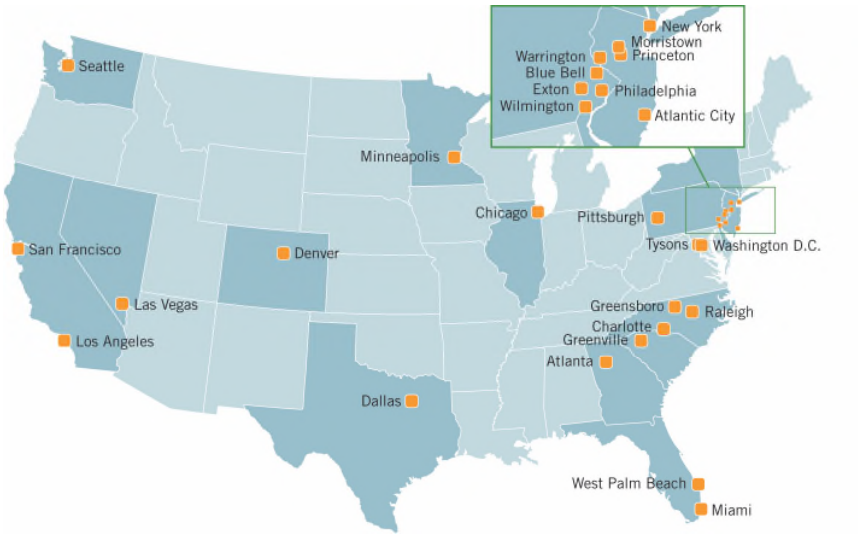
Our team works with clients to assess their exposure to the European Union's General Data Protection Regulation (GDPR) and design policies and procedures to mitigate risks. We use our detailed knowledge of EU data protection law, coupled with our understanding of the unique challenges it poses to U.S.-based corporations, to create pragmatic, actionable, tailored plans to achieve GDPR compliance.

CCPA Compliance

We help companies prepare for The California Consumer Privacy Act (CCPA). In effect as of January 2020, the CCPA has changed the way companies both inside and outside the state manage consumers' personal data by conferring a new set of rights on consumers and a new set of responsibilities on the companies that handle their data. We help clients determine their exposure, catalog the data they collect and how it is used, and update their privacy policies, procedures and websites to bring them into compliance with this new law.

The Fox Difference

Fox Rothschild is a leader. We've been named to the Law Firms Best at Cybersecurity Honor Roll by BTI, a respected provider of client-based data for the legal industry. When you choose Fox, you get Privacy & Data Security attorneys who are nationally recognized:



- Team members who are CIPP/US, CIPP/E, and CIPM certified by the International Association of Privacy Professionals and CDPO certified by the Professional Evaluation and Certification Board.
- Partners named Trailblazers in Cybersecurity Law by the *National Law Journal*.
- Chambers-ranked attorneys.

Our lawyers are frequent speakers on safeguarding sensitive information and new developments in privacy. The team includes attorneys who are frequently quoted on issues of privacy and data security by national media outlets such as *The Economist, The Wall Street Journal, The New York Times, Forbes, The Huffington Post and Compliance Week.*

We're also one of few firms in the country that has its own Chief Privacy & HIPAA Compliance Officer.

Part of a law firm with 950 attorneys in offices coast-to-coast, Fox Rothschild's Privacy & Data Security team delivers the service and focus of a boutique with the reach and resources of a national law firm.

Key Contacts

ODIA KAGAN
Partner and Chair of GDPR Compliance & International Privacy
okagan@foxrothschild.com

ELIZABETH LITTEN
Partner and Chief Privacy & HIPAA Compliance Officer | Co-Chair, Privacy & Data Security Practice
elitten@foxrothschild.com

MARK G. MCCREARY
Partner | Co-Chair, Privacy & Data Security Practice
mmccreary@foxrothschild.com

State Consumer Data Privacy Protection Laws Snapshot

Following California's adoption of the California Consumer Privacy Act (CCPA) in 2018, lawmakers in multiple states have proposed, and in some cases enacted, similar laws aimed at safeguarding consumer data.

The following table provides a summary of the status, and key provisions in those laws as of DATE.

LEGISLATIVE HISTORY

State	Status	Effective Date (if applicable)	Link to Text
Alabama	Bill	10/1/2022	HB216
Alaska	Bill		SB 116 and HB 159 (identical bills)
Arizona	Bill		HB 2865
California	Passed	1/1/2020	AB 375
California	Passed	01/01/2023	Prop 24
Colorado	Bill		SB21-190
Connecticut	Bill	01/01/2023	SB 893
Delaware			
Florida	Bill	01/01/2022	HB 969
Florida	Died in Senate		SB 1734
Hawaii	Died in Committee		SB 418
Hawaii	Regular session adjourned; carryover pending		HB 2572
Illinois	Bill		HB 3358
Illinois	Bill		HB 3910
Illinois	Bill	7/31/2021	SB 2330
Illinois	Bill		SB 2263
Illinois	Bill		HB 5603
Kentucky	Died in Committee		HB 408
Louisiana	Adopted		HR 249
Maine	Enacted	7/1/2020	SB 275
Maryland	Died in Committee		SB 613
Maryland	Regular session adjourned; carryover pending		HB 1656
Maryland	Bill		SB 0930
Massachusetts	Study Order Issued		S 120
Massachussets	Bill		SD 1726
Minnesota	Regular session adjourned; carryover pending		"MN HF 1030 (Same as SF 433)"
Minnesota (HF 1492)	Bill		HF 1492

State	Status	Effective Date (if applicable)	Link to Text
Minnesota HF (36)	Bill		HF 36
Mississippi	Died in Committee		SB 2612
Nebraska	Bill		LB 746
Nevada	Passed	10/1/2019	SB 220
New Hampshire	Regular session adjourned; carryover pending	1/1/2021	HB 1680
New Jersey	Bill		S 269
New Jersey	Bill		A 3255
New Jersey	Bill		A3283
New Mexico	Died in Chamber		SB 176
New York	Bill		SB 224
New York	Bill		SB 5642
New York	Bill		SB 567
New York	Bill		A6042
North Dakota	Passed		HB 1485
Oklahoma (HB 1130)	Bill	11/1/2021	HB 1130
Oklahoma (HB 1602)	Bill		HB 1602
Pennsylvania	Died in Committee		HB 1049
Pennsylvania	Bill		HB 1126
Texas	Bill	9/1/2021	HB3741
Utah (SB 249)	Failed		S.B. 249
Utah (SB 200)	Failed		S.B. 200
Virginia	Passed	01/01/2023	H2307
Washington (SB 5062)	Died in Committee		SB5062
Washington (HB 1433)	Died in Committee	7/31/2022	HB1433
West Virginia	Bill		HB 3159

BUSINESSES COVERED

State	Minimum revenue to meet definition of covered business	# of consumers to meet definition of covered business	% annual revenue to meet definition of covered business
Alabama	No	No	No
Alaska	$25 million	100,000	No
Arizona	$25 million	100,000	35% of gross revenue from sale of personal information (AND processes or controls personal information of at least 25,000 consumers)
California (CCPA)	$25 million	50,000+	50%
California (CPRA)	$25 million	50,000	50%
Colorado	No	100,000	No
Connecticut	No	100,000	50% of gross revenue from sale of personal data (AND processes or controls at least 25,000 consumers' personal data)
Nevada	No, per Nevada's previously passed law 603A	No, per Nevada's previously passed law 603A	No, per Nevada's previously passed law 603A
Florida (HB 969)	$50 million	50,000	50%
Florida (SB 1734)	No	100,000	50%
Hawaii (SB 418)	No	No	No
Hawaii (2572)	No	No	No
Illinois (HB 3358)	None	>50,000	50%
Illinois (HB 3190)	$25 million	50,000	50%
Illinois (SB 2330)	No	50,000+	50%
Illinois (SB 2263)	No	100,000+	50% and processes or controls personal data of 25,000 consumers or more
Illinois (HB 5603)	$25 million	500,000+	50%
Kentucky	$25 million	50,000	50%
Louisiana	No	No	No
Maine	No	No	No
Maryland (SB 613)	No	100,000+	50%
Maryland (HB 1656)	In excess of $25 million	50,000+	50%
Maryland (SB 0930)	$25 million	100,000	50%
Massachusetts (SD 1726)	$10 million earned through 300 or more transactions	10,000	No
Minnesota (HF 1492)	No	100,000	25% of gross revenue from sale of personal data (AND process or control personal information of at least 25,000 consumers)
Minnesota (HF 36)	$25 million	50,000	50%
Mississippi (SB 2612)	$10 million	50,000	50%
Nebraska	Over $10 million	50,000+	50%
Nevada	No, per Nevada's previously passed law 603A	No, per Nevada's previously passed law 603A	No, per Nevada's previously passed law 603A
New Hampshire	In excess of $25 million	50,000+	50%
New Jersey (S 269)	No	No	50%
New Jersey (A 3255)	$25 million	50,000	50%

State	Minimum revenue to meet definition of covered business	# of consumers to meet definition of covered business	% annual revenue to meet definition of covered business
New Jersey (A 3283)	No	No	No
New Mexico	No	No	No
New York (SB 224)	No	No	No
New York (SB 5642)	No	No	No
New York (SB 567)	$50 million	100,000	50%
New York (A6042)	No	No	No
North Dakota	No	No	No
Oklahoma (HB 1130)	No	No	No
Oklahoma (HB 1602)	$10 million	50,000 (alone or in combination with others)	25%
Pennsylvania	$10 million	50,000	50%
Pennsylvania (HB 1126)	$10 million	50,000	50%
Texas	$25 million	5,000	50%
Utah (SB 249)	$25 million	50,000	50%
Utah HB 200	No	No	No
Virginia (HB 473)	No	100,000	50% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more
Virginia (HB 2307) (CDPA)	No	100,000	50% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more
Washington (SB 5062)	None	100,000	25% of gross revenue from the sale of personal data AND processes or controls personal data of 25,000 consumers or more
Washington (HB 1433)	$10 million through 300 or more transactions	1,000	No
West Virginia	$25 million	50,000	50%

CONSUMER PROTECTIONS

State	Access to Personal Info Collected	Access to Personal Information Shared	Right to Correction	Right to Deletion	Right to Data Portability
Alabama	Yes	No (categories)	No	Yes	Yes
Alaska	Yes	Yes	No	Yes	Yes
Arizona	Yes	No (categories)	Yes	Yes	Yes
California (CCPA)	Yes	Yes	No	Yes	Yes
California (CPRA)	Yes	Yes	Yes	Yes	Yes
Colorado	Yes	Yes	Yes	Yes	Yes
Connecticut (SB 893)	Yes	Yes	Yes	Yes	Yes
Nevada	Yes, per Nevada's previously passed law 603A	No	No	No	No
Florida (HB 969)	Yes	Yes	Yes	Yes	Yes
Florida (SB 1734)	Yes	Yes	Yes	Yes	No
Hawaii (SB 418)	Yes	Yes	No	Yes	No
Hawaii (HB 2572)	Yes	Yes	No	Yes	Yes
Illinois (HB 3358)	No	Yes	No	No	No
Illinois (HB 3190)	Yes	Yes	No	Yes	Yes
Illinois (SB 2330)	Yes	Yes	Yes	Yes	Yes
Illinois (SB 2263)	Yes	Yes	Yes	Yes	Yes
Illinois (HB 5603)	Yes	Yes	No	Yes	Yes
Kentucky	No	No	No	No	No
Louisiana	No	No	No	No	No
Maine	No	No	No	No	No
Maryland (SB 613)	Yes	No	No	Yes	Yes
Maryland (HB 1656)	Yes	Yes	No	Yes	No
Maryland (SB 0930)	Yes	Yes	No	Yes	Yes
Massachusetts (SD 1726)	Yes	Yes	Yes	Yes	Yes
Minnesota (HF 1492)	Yes	Yes	Yes	Yes	Yes
Minnesota (HF 36)	Yes	No (categories)	No	Yes	No
Mississippi	Yes	No (categories)	No	Yes	No
Mississippi (SB 2612)	Yes	No	No	Yes	No
Nebraska	Yes	Yes	No	Yes	No
New Hampshire	Yes	Yes	No	Yes	Yes
New Jersey (S 269)	Yes	Yes	Yes	No	No
New Jersey (A 3255)	Yes	Yes	No	Yes	No
New Jersey (A 3283)	Yes	Yes	Yes	Yes	Yes
New Mexico	Yes	Yes	No	Yes	Yes
New York (SB 224)	Yes	Yes	No	No	No

State	Access to Personal Info Collected	Access to Personal Information Shared	Right to Correction	Right to Deletion	Right to Data Portability
New York (SB 5642)	Yes	Yes	Yes	Yes	No
New York (SB 567)	Yes	Yes	No	No	No
New York (A6042)	Yes	Yes	No	Yes	No
North Dakota	No	No	No	No	No
Oklahoma (HB 1130)	No	No	No	No	No
Oklahoma (HB 1602)	Yes	Yes	No	Yes	Yes
Pennsylvania	Yes	Yes	No	Yes	No
Pennsylvania (HB 1126)	Yes	No	No	Yes	No
Texas	Yes	No (categories)	Yes	Yes	Yes
Utah (SB 249)	Yes	Yes	No	Yes	No
Utah (SB 200)	Yes	Yes	No	Yes	Yes
Virginia	Yes	Yes	Yes	Yes	Yes
Washington (SB 5062)	Yes	Yes	Yes	Yes	Yes
Washington (HB 1433)	Yes	Yes	Yes	Yes	Yes
West Virginia	Yes	Yes	Yes	Yes	Yes

CONSUMER RIGHTS & ENFORCEMENT

State	Opt Out	Children	Private right of action	Vendor Provisions
Alabama	Yes	Yes	Yes	Yes
Alaska	Yes	Yes	Yes	Yes
Arizona	No	No	No	Yes
California (CCPA)	Yes	Yes	Yes	Yes
California (CPRA)	Yes	Yes	Yes	Yes
Colorado	Yes	Yes		Yes
Connecticut (SB 893)	Yes	Yes	No	Yes
Nevada	Yes	No	None	No
Florida (HB 969)	Yes	Yes	Yes	Yes
Florida (SB 1734)	Yes	Yes	No	Yes
Hawaii (SB 418)	Yes	Yes	None	No
Hawaii (HB 2572)	Yes	Yes	No	Yes
Illinois (HB 3358)	Yes	No	No	No
Illinois (HB 3190)	Yes	Yes	Yes	Yes
Illinois (SB 2330)	Yes	No	Yes	Yes
Illinois (SB 2263)	No	Yes	No	Yes
Illinois (HB 5603)	Yes	Yes	No	Yes
Kentucky	Yes	Yes	No	No
Louisiana	No	No	No	No
Maine	Yes (referred to as Opt In)	No	No	No
Maryland (SB 613)	Yes	Yes	No	Yes
Maryland (HB 1656)	Yes	Yes	No	No
Maryland (SB 0930)	Yes	No	Yes	No
Massachusetts (S 1726)	Yes (annual opt-in)	Yes	Yes	Yes
Minnesota (HF 1492)	Yes	Yes	No	Yes
Minnesota (HF 36)	Yes	Yes	Yes	Yes
Mississippi	Yes	Yes	Yes	Yes
Mississippi (SB 2612)	Yes	Yes	Yes	Yes
Nebraska	Yes	Yes	No	Yes
New Hampshire	Yes	Yes	Yes	Yes
New Jersey (S 269)	Yes	No	Yes	Yes
New Jersey (A 3255)	Yes	No	Yes	No
New Jersey (A 3283)	No	No	No	Yes
New Mexico	Yes	Yes	Yes	Yes
New York (SB 224)	Yes	No	Yes	Yes
New York (SB 5642)	Yes	No	Yes	Yes
New York (SB 567)	Yes	Yes	Yes	yes
New York (A6042)	No	No	Yes	Yes
North Dakota	No	No	Yes	No
Oklahoma (HB 1130)	No	No	No	No
Oklahoma (HB 1602)	Yes (opt-in for sales)	No	No	Yes
Pennsylvania	Yes	Yes	Yes	No

State	Opt Out	Children	Private right of action	Vendor Provisions
Pennsylvania (HB 1126)	Yes	Yes	Yes	Yes
Texas	No	No	No	Yes
Utah (SB 249)	Yes	No	Yes	Yes
Utah (SB 200)	Yes	Yes	Yes	Yes
Virginia	No	Yes	Yes	Yes
Washington (SB 5062)	Yes	Yes	Yes	Yes
Washington (HB 1433)	Yes (annual opt-in)	Yes	Yes	Yes
West Virginia	Yes	Yes	Yes	Yes

Detailed State-by-State Analysis

Alabama

Alabama Consumer Privacy Act

- Legislative Status: Referred to Technology and Research Committee
- Link to Text: HB 216
- Effective Date: October 1, 2022

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared[1]		✓
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability[2]	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children[3]	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means an individual who is a resident of Alabama; however identified, including by any unique identifier.

- ***Personal Information*** means information that identifies, relates to, describes, can be associated with or could reasonably be linked to, directly or indirectly, a particular consumer or household. This includes, but is not limited to:

  - Identifiers (e.g., name, address, usernames, email addresses, account names, Social Security numbers, driver's license numbers, etc.)

[1] Consumers may access the categories of information shared or sold, but not the information.
[2] While portability is only required if the disclosure is given electronically, electronic delivery is at the consumer's option if the consumer does not have an account with the business. *See* §9(a)(2).
[3] Persons under 18 must opt in.

- Online identifiers (e.g. email, IP address, etc.)
- Physical characteristics
- Characteristics of protected classifications under Alabama or federal law
- Commercial information (e.g. records of personal property, products or services purchased, etc.)
- Biometric information
- Internet or network activity
- Geolocation data
- Audio/electronic/visual/thermal/olfactory information
- Professional or employment-related information
- Education information that is not publicly available personally identifiable information under the federal Family Educational Rights and Privacy Act; or
- Inferences drawn from any of the above to create a "profile about a consumer" that reflect preferences, psychological trends, behaviors, etc.

❖ ***Business*** means either:

- A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, and that does business in the state of Alabama; or
- An entity that controls or is controlled by a business meeting the requirements above and that shares common branding with the business.

Enforcement

- Violations of this act by a business, service provider or any other person shall be deemed a violation of the Deceptive Trade Practices Act, § 8-19-1 et. seq. Code of Alabama 1975, and shall be subject to the same penalties as provided in that act.
- The Attorney General may bring actions under the Deceptive Trade Practices Act.
- ***Private Right of Action***[4]
  - Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's failure to implement and maintain reasonable personal information security procedures and practices appropriate to the nature of the information may institute a civil action for any or all of the following: damages, injunctive or declaratory relief, and any other relief the court deems proper.
  - Prior to imitating an action for statutory damages, a consumer shall provide written notice of the alleged violations, and the business will have 30 days to cure. If cured, no action may be brought for statutory damages.
  - No notice is required for a consumer to initiate an action solely for actual pecuniary damages suffered as a result of violations of this act.
  - This act does not provide for a private right of action under any other law.

Data Safe Harbors

- This act does not apply to:
  - Nonprofits or governmental entities
  - Publicly available information

[4] The act seems to require a consumer give the Attorney General 30-day notice; however, the subsection reference is incorrect.

- Information that is collected by an entity governed under HIPAA
- Information used to create or reported in a consumer report and complying with the Fair Credit Reporting Act and solely used under that act
- Personal information collected, processed, sold, or disclosed under:
  - Gramm-Leach-Bliley Act (the "GLBA) of 1999 and its regulations; or
  - The federal Driver's Privacy Protection Act of 1994
- De-identified or aggregate consumer information

❖ This act does not interfere with a business's ability to

- Comply with
  - Applicable federal, state, or local laws; or
  - A civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, or local authority
- Cooperate with a law enforcement agency concerning conduct that the business, a service provider, or a third party reasonably and in good faith believes may violate other applicable federal, state, or local laws
- Pursue or defend against a legal claim
- Collect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate consumer information
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of Alabama
- Retain information after a deletion request to detect a security incident, protect against malicious, deceptive, fraudulent or illegal activity; or prosecute those responsible for the illegal activity described above

- Violate an evidentiary privilege under state law

❖ This act does not require a business to:

- Retain a consumer's personal information that was collected for a one-time transaction if the information is not sold or retained in the ordinary course of business
- Re-identify or otherwise link any data, that in the ordinary course of business, is not maintained in a manner that would be considered personal information
- Comply with unverified requests

❖ This act does not require a business or service provider to comply with a consumer request to delete information if the business or service provider needs to retain the consumer's personal information to:

- Comply with a consumer's opt-out request, if used solely for that purpose;
- Complete the transaction for which the information was collected;
- Provide a good or service requested by the consumer in the context of the ongoing business relationship;
- Perform under a contract between the business and the consumer;
- Detect a security incident; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such illegal activity;
- Debug, identify and repair or remove errors that impair existing intended functionality;
- Exercise free speech or ensure the right of another consumer to exercise the right of free speech or another right afforded by law;
- Comply with a legal obligation;

- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;

- Otherwise use the consumer's personal information internally and in a lawful manner that is compatible with the context in which the consumer provided the information; or

- Engage in peer-reviewed scientific, historical, or statistical research that is in the public interest and that adheres to all other applicable ethics and privacy laws, provided that:

    - The business's deletion is likely to render impossible or seriously impair the achievement of the research; and

    - The consumer has previously provided to the business informed consent.

Vendor Provisions

❖ A business is not liable for a service provider's violations of this act provided the business:
  - (1) Does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation at the time of disclosure; and

  - (2) Engages the service provider in a written contract that

    - (i) Prohibits the service provider from

      - (a) Selling the personal information;

      - (b) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract or as otherwise prohibited by this act, including retaining, using, or disclosing the personal information for commercial purpose other than providing the services provided in the contract;

- (c) Retaining, using, or disclosing the information outside the direct business relationship between the service provider and the business.

- (ii) Includes a certification made by the service provider that it understands the restrictions in item (i) and will abide by them.

❖ A third party shall not sell personal information about a consumer that was sold to the third party by a business unless the consumer received explicit notice of the sale and is provided an opportunity to opt out.

❖ A service provider is not liable under this act for the obligations of a business for which it provides services as set forth in this act.

Alaska

Alaska Consumer Protection Act

- Legislative Status: Introduced March 31, 2021
- Link to Text: SB 116 and HB 159 (identical bills)

Alaska's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓
Opt In	✓	

Key Definitions

- ***Business*** means either:
  - (A) A for-profit legal entity that:
    - (1) Collects or has collected consumers' personal information, or on the behalf of which that information is collected, alone or jointly with others, determines the purposes and means of processing consumers' personal information;
    - (2) Does business in the state of Alaska; and
    - (3) Satisfies one or more of the following thresholds: (i) had annual gross revenues of $25 million or more in the year 2022 or in any year thereafter; (ii) in the most recent completed calendar year, alone or in combination, bought or disclosed the personal information of 100,000 or more persons or households; (iii) sold the personal information of a consumer, household, or device in the last 365 days; or

- (4) An entity controlled or being controlled by a business that meets a threshold in (A) of this paragraph and shares common branding, such as a shared name, service mark, or trademark, with the business.

❖ ***Collect*** includes buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means, actively or passively receiving information from the consumer, or by observing the consumer's behavior.

❖ ***Consumer*** means a resident of the state, however identified, including by any unique identifier, who is physically present in the state with the intent to remain indefinitely in the state under the requirements of AS 01.10.055.

❖ ***Personal Information*** means (A) *information that identifies*, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

- "Information that identifies" includes

  - (i) A real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, electronic mail address, account name, Social Security number, driver's license number, or passport number;

  - (ii) Characteristics of protected classifications under state or federal law;

  - (iii) Any category of personal information as defined in AS 45.48.090;

  - (iv) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

  - (v) Biometric information, which includes an individual's physiological, biological, or behavioral characteristics; deoxyribonucleic acid, that can be used, singly or in combination with other identifying data, to establish individual identity; imagery of the retina, fingerprints, face, vein patterns, or voice recordings that can be used as an identifier template; keystroke patterns or rhythms; or sleep, health, or exercise data;

- (vi) Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
- (vii) Geolocation data, including precise geolocation data;
- (viii) Audio, electronic, visual, thermal, olfactory, or similar information;
- (ix) Professional or employment information;
- (x) Education information that is not publicly available, personally identifiable information as defined in 20 U.S.C. 1232g; 34 C.F.R. Part 99 (Family Educational Rights and Privacy Act);
- (xi) Inferences drawn from any of the information identified in this subparagraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

➢ Personal Information does *not* include publicly available information that is lawfully made available from federal, state, or local government records; biometric information as described in (A) of this paragraph, collected by a business without a consumer's knowledge is not considered publicly available information, or consumer information that is de-identified or aggregated.

Enforcement

❖ ***Department of Law***

o The Alaska Department of Law would enforce the Act. Violations would be deemed an "unfair or deceptive act or practice" under Alaskan state law, and could result in fines ranging from $1,000 to $25,000 for each violation.

❖ ***Private Right of Action***

o The Act also would create a limited private right of action for any consumer whose personal information is subjected to "unauthorized access, destruction, use,

modification, or disclosure." The Act defines such a violation as an "ascertainable loss of $1 or of an amount proven at trial, whichever is greater."

Data Safe Harbors

There are several safe harbors and exceptions under the Alaska Consumer Protection Act.

- The Act does not apply to the following:
  - Protected health information that is collected by a covered entity or business associate governed by HIPAA;
  - A Covered Entity governed by the privacy, security, and breach notification rules established in accordance with HIPAA;
  - Information collected as part of a clinical trial subject to the Federal Policy For The Protection Of Human Subjects
  - Vehicle or ownership information retained or shared between a new motor vehicle dealer and the motor vehicle manufacturer, if the information is shared for the purpose of or in anticipation of effectuating a vehicle repair covered by a vehicle warranty or recall conducted under 49 U.S.C. 30118 - 30120, provided that the new motor vehicle dealer or vehicle manufacturer does not sell, share, or use the information for any other purpose.
- A person may disclose a consumer's personal information to:
  - Comply with federal, state, or local law;
  - Comply with a civil, criminal, or regulatory inquiry or an investigation, subpoena, or summons by federal, state, or local authorities;
  - Cooperate with law enforcement agencies concerning conduct or activity that the person reasonably and in good faith believes may violate federal, state, or local law;
  - Exercise or defend legal claims;

- Collect, use, retain, sell, or disclose, de-identified or aggregated consumer information.

❖ Notwithstanding other provisions of the Act, a business may collect or sell a consumer's personal information if the commercial conduct takes place wholly outside the state. For the purpose of this subsection, commercial conduct takes place wholly outside the state if:

- The business collected the information while the consumer was outside the state; this does not include the storage of personal information, including on a personal device, while the consumer is in the state and collection when the consumer and stored information subsequently leave the state;
- No part of the sale of the consumer's personal information occurred in the state; and
- No personal information collected while the consumer was in the state was sold.

❖ Excluding the right to file an action for a violation of AS 45.49.120, the Act does not apply to:

- Certain activity that is subject to the Fair Credit Reporting 18 Act; or
- Personal information processed under the GLBA.

❖ Certain information collected by a business is exempt from this chapter until January 1, 2024, if the information:

- Is collected through a person's:
  - (A) Job application to the business;
  - (B) Service as an employee, officer, or director of the business;
  - (C) Ownership of the business;
  - (D) Service as a dentist licensed under AS 08.36, physician licensed under AS 08.64, or a psychologist licensed under AS 08.86; or

- (E) Work as a contractor for the business; and

➢ Consists only of:

- (A) Personal information used solely within the context for which it was collected;
- (B) Emergency contact information used solely for the purpose of having an emergency contact on file; or
- (C) Personal information retained solely to administer benefits.

❖ Certain personal information contained in written or verbal communication or a transaction between a business and a consumer is exempt from this chapter if:

➢ The consumer is a natural person acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency; and

➢ The communication or transaction occurs solely within the context of the business's exercising due diligence regarding a product or service, or to receive a product or service from or provide a product or service to the company, partnership, sole proprietorship, nonprofit, or government agency.

❖ A requirement under this chapter does not apply if

➢ Compliance with the requirement would violate an evidentiary privilege under state law;

➢ The business provides personal information as part of privileged communication to a person covered by an evidentiary privilege;

➢ The right or obligation would adversely affect a right of another consumer;

➢ The right or obligation would infringe on the noncommercial activity of a person or entity exercising rights under art. I, sec. 5, Constitution of the State of Alaska.

Vendor Provisions

- Third parties that receive consumer personal information as part of a transaction in which the third party assumes control of all or part of the business and the third party decides to change how it uses or shares the consumer's personal information in a manner that is materially inconsistent with the promises made at the time of collection, shall notify the consumer before the change. The notice must ensure that existing consumers can easily exercise consumers' rights under the Act.

- A service provider may not:

  - Retain, use, or disclose personal information received from a business for any purpose other than to perform the services specified in a written contract with the business;

  - Combine personal information received from a business with personal information the service provider receives from other sources, unless otherwise provided in regulations adopted by the Attorney General; or

  - Disclose personal information received from a business to any other person without first:

    - Receiving written consent of the business to disclose the personal information to the other person; and

    - Entering into a written contract with the other person that prohibits the other person from engaging in conduct prohibited under this section.

Arizona

Personal data; processing; security standards

- Legislative Status: Referred to Commerce Committee and Read in House Second Time
- Link to Text: HB 2865

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared[5]		✓
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out		✓
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is an Arizona resident and who is acting only in an individual, noncommercial or household context.
- ***Personal Information*** or ***Personal Data*** means information that is or can reasonably be linked to an identified or identifiable natural person. This include sensitive data.
- ***Personal Information*** or ***Personal Data*** does not include de-identified or public information.
- ***Controller*** means the natural or legal person that, alone or jointly with others, determines the purposes and means of processing personal data.

Enforcement

[5] The controller must give the categories of shared personal data, but it is not required to provide the data itself.

- The Attorney General may bring actions in the name of this state, or as parens patriae, on behalf of persons residing in this state, to enforce this article.
- A controller or processor violates this article if it fails to cure any alleged breach of this article within thirty (30) days after receiving notice of the alleged noncompliance.
- The Attorney General may seek injunctions or civil penalties up to $2,500 for each violation and $7,500 for each intentional violation.
- This article supersedes and preempts any other state or local law or regulation.
- This act does not provide for a ***Private Right of Action***.

Data Safe Harbors

- This act applies to legal entities that
  - (1) Have a gross annual revenue of at least $25 million;
  - (2) Conduct business within or produce products or services that are intentionally targeted to residents of Arizona
  - (3) And either:
    - Controls or processes data of at least one hundred thousand (100,000) consumers; or
    - Derives over 35% of its gross revenue from the sale of personal information and processes or controls personal information of at least 25,000 consumers
- This act does not apply to:
  - State or local governments
  - Publicly available information
  - Personal information sets to the extent they are governed by:

- HIPAA;
- The Health Information Technology for Economic and Clinical Health Act; or
- The Gramm-Leach-Bliley Act.

➢ Data sets maintained for employment records purposes.

➢ Businesses and activities covered by the Fair Credit Reporting Act

➢ De-identified data

❖ This act does not interfere with a controller or processors ability to

➢ Comply with

- Applicable federal, state, or local laws; or
- A civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, or local or other governmental authority

➢ Cooperate with a law enforcement agency concerning conduct that the business, a service provider, or a third party reasonably and in good faith believes may violate other applicable federal, state, or local laws or regulations

➢ Investigate or defend against a legal claim

➢ Prevent or detect identity theft, fraud, or other criminal activity or verify identities

➢ Violate an evidentiary privilege under state law

❖ This act does not require a business to:

➢ Retain a consumer's personal data that was collected for a one-time transaction if the information is not in the a manner that would be considered personal data

➢ Re-identify or otherwise link any data, that in the ordinary course of business, is not maintained in a manner that would be considered personal information

- Comply with unverified requests

❖ This act requires a controller to delete collected or processed personal data upon a verified consumer request if:

- The personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed;
- The processing requires consent and the consumer has withdrawn consent, and there are no business purposes for the processing;
- The personal data must be deleted to comply with a legal obligation to which the controller is subject;
- The controller is required to certify when the deletion was completed; or
- The personal data has been unlawfully processed.

❖ The act does not require the controller to delete personal data if it is needed to:

- Complete the transaction for which the information was collected;
- Provide a good or service requested by the consumer in the context of the ongoing business relationship;
- Perform under a contract between the collector and the consumer;
- Detect or respond to a security incident; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such activity;
- Exercise free speech
- Comply with a legal obligation;
- To aid public interest in the area of public health, if the processing is both of the following:

- Subject to suitable and specific measures to safeguard the rights of the consumer; and

- Under the responsibility of a professional subject to confidentiality obligations under a federal, state, or local regulations.

➢ To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; or

➢ Archive in the public interest or scientific, historical, or statistical research purposes if deleting such information is likely to render impossible or seriously impair the achievement of the processing

Vendor Provisions

❖ A controller is presumed to have sold personal data if there is an exchange of personal data and if the contract terms with the third party do not limit the use of personal information by the third party

❖ A controller or processor that discloses personal data to a third party controller or processor in compliance with this article is not liable for a violation by the third-party recipient unless the disclosing controller or processor had actual knowledge that the recipient intended to violate this act at the time of disclosing

❖ A third-party recipient that receives personal data from a controller or processor is not liable under this article for the obligations of a controller or processor for which it provides services

❖ If more than one controller or processor, or both a controller and a processor, involved in the same processing are in violation of the article, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties

California

California Consumer Privacy Act, AB 375

- Legislative Status: Passed
- Effective Date: 1/1/2020
- Link to Text: AB 375
- Passed Amendments:
  - AB 713; Approved and Chaptered as of 09/25/2020
  - AB 1281; Approved and Chaptered as of 09/29/20
- See the below chart for additional pending amendments.

California's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is defined as a natural person who is a California resident.

- ***Personal Information*** is defined as information that identifies, relates to, describes, is associated with, or could reasonably be linked, directly or indirectly with a customer, and includes:

  - Name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers

- Personal information like address, signature, Social Security number, telephone number, any identification numbers, any banking identification numbers, and employment history
- Protected classifications under California or federal law
- Commercial information, like personal property records, products or services purchased or considered, or other purchasing or consuming histories or tendencies
- Biometric information
- Internet or other electronic network activity information, including browsing history and information regarding a consumer's interaction with an Internet Web site, application, or advertisement
- Geolocation data
- Audio, electronic, visual, or similar information
- Professional or employment-related information
- Education information
- Inferences drawn about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, and intelligence

**Personal information does not include publicly available information.*

- ***Business*** is defined as a for profit legal entity that does business in the state of California and collects consumers' personal information, or on the behalf of which such information is collected, determines the purposes and means of processing consumers' personal information. The business must satisfy one or more of the following thresholds:
  - Has annual gross revenues in excess of $25 million

- Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices

- Derives 50% or more of its annual revenues from selling consumers' personal information

- ***Business*** is also defined as an entity that controls or is controlled by a business, as defined above, and shares common branding with the business.

Enforcement

- ***Enforcement***

  - The Attorney General may bring a civil action to recover penalties.

- ***Private Right of Action***

  - A consumer may bring a civil action for any of the following:

    - To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater; or

    - Injunctive or declaratory relief.

Data Safe Harbors

- Personal information collected by a covered entity governed by the Confidentiality of Medical Information Act or governed by the privacy, security and breach notification rules established under HIPAA

- Sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report

- Personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA)

- Personal information collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994
- To comply with federal, state, or local laws
- Comply with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state or local authorities
- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law
- Exercise or defend legal claims
- Collect, use, retain, sell or disclose consumer information that is de-identified or in the aggregate consumer information
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside California
- Collect, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency or furnisher of information who provides information for use in a consumer report pursuant to the Fair Credit Reporting Act.
- Retain or share vehicle and owner information for the purpose of vehicle repairs covered by a warranty or a recall-related repairs
- Collect personal information, emergency contact information and beneficiary information from a job applicant, employee, owner, director, officer, medical staff member or contractor of that business until Jan. 1, 2021.

Vendor Provisions

- The CCPA prohibits a third party from selling personal information about a consumer that was sold to the third party by a business, unless the consumer received explicit notice and is provided an opportunity to exercise the right to opt out.

California

California Privacy Rights Act (CPRA)
NOTE: The CPRA will replace the CCPA when it takes effect.

- Legislative Status: Passed as Proposition 24 on Nov. 3, 2020. Effective January 1, 2023
- Link to Text: CPRA

California's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction	✓	
Opt In	✓	

Key Definitions

- ***Business*** means either:

  - (1) A for-profit legal entity that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of California, and that satisfies one or more of the following thresholds:

    - Has annual gross revenues in excess of $25 million, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185;

    - Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices;

- Derives 50% or more of its annual revenues from selling consumers' personal information; or

➢ (2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business.

❖ ***Consumer*** means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

❖ ***Person*** means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

❖ ***Personal Information*** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

➢ Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.

➢ Any categories of personal information described in subdivision (e) of Section 1798.80.

➢ Characteristics of protected classifications under California or federal law.

➢ Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

➢ Biometric information.

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

- Geolocation data.

- Audio, electronic, visual, thermal, olfactory, or similar information.

- Professional or employment-related information.

- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

❖ ***Personal information*** does not include:

- publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

- consumer information that is de-identified or aggregate consumer information.

❖ ***Service Provider*** means a for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

❖ ***Enforcement***

➢ ***Attorney General***

- Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.
- The Attorney General may bring civil actions for violations.

➢ ***Private Right of Action***

- Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
  - To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.
  - Injunctive or declaratory relief.
  - Any other relief the court deems proper.

Data Safe Harbors

❖ Compliance with federal, state, or local laws or court order or subpoena to provide information.

❖ Compliance with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

❖ Cooperation with law enforcement agencies.

- Cooperation with certain government agency requests for emergency access to consumer's personal information if a natural person is at risk or danger of death or serious physical injury.

- To exercise or defend legal claims.

- To collect, retain, sell, share, or disclose consumers' personal information that is de-identified or aggregate consumer information.

- To collect or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California.

- Where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

- Health information collected by a covered entity or business associate

- HIPAA Covered Entities.

- Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects.

- Additionally, a business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

  - Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;

- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- Comply with a legal obligation;
- Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Vendor Provisions

- A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

California has several amendments to the CCPA and CPRA now pending. The chart below provides and overview of this legislation.

Bill	Title	Status	Summary
AB 335	An act to amend Section 1798.145 of the Civil Code, relating to privacy	Introduced Jan. 27, 2021. Apr. 8, 2021 referred to Committee on APPR.	Exempts certain vessel information or ownership information retained or shared between vessel dealers and manufacturers from the CCPA and CPRA right to opt out.
AB 825	An act to amend Sections 1798.29, 1798.81.5, and 1798.82 of the Civil Code, relating to information privacy.	Introduced Feb. 16, 2021. Apr. 8, 2021, referred to Committee on APPR.	Amends the definition of personal information to include genetic data.
AB 1490	An act to amend Sections 1798.199.10 and 1798.199.15 of the Civil Code, relating to privacy.	Introduced Feb. 19, 2021. Apr. 8, 2021, referred to Committee on APPR.	This bill would require members of the board of the California Privacy Protection Agency to additionally have qualification, experience, and skills in consumer rights.

SB 746	An act to amend Section 1798.130 of, and to add Section 1798.111 to, the Civil Code, relating to privacy.	Introduced Feb. 19, 2021.	This bill would grant a consumer the right to request that a business disclose to the consumer whether or not the business uses personal information collected about the consumer for a political purpose, as defined.

Colorado

Colorado Privacy Act

- Legislative Status: Introduced on March 19, 2021
- Link to Text: SB21-190

Colorado's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- The Colorado Privacy Act applies to legal entities that conduct business or produce products or services that are intentionally targeted to Colorado residents and that either: (1) control or process personal data of more than 100,000 consumers per calendar year; or (2) derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers; and (3) does not apply to personal data governed by listed state and federal laws, listed activities, and employment records.

- ***Consumer*** means an individual who is a Colorado resident acting only in an individual or household context; and does not include an individual acting in a commercial or employment context.

- ***Personal Data*** means information that is linked or reasonably linkable to an identified or identifiable individual; and does not include de-identified data or publicly available information.

- ***Sensitive Data*** means:

- (a) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;
- (b) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or
- (c) the personal data of a known child.

Enforcement

❖ ***Attorney General***

- The Attorney General and district attorneys have exclusive authority to enforce this part by bringing an action in the name of the state or as parens patriae on behalf of persons residing in the state to enforce this part, including seeking an injunction to enjoin a violation of this part.

❖ ***No Private Right of Action***

Data Safe Harbors

❖ The obligations imposed on controllers or processors under the Act do not restrict a controller's or processor's ability to:

- Comply with Federal, state or local laws, rules, or regulations;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by Federal, state, local or government authorities;
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate Federal, state, or local law;
- Investigate, exercise, prepare for, or defend legal claims;
- Conduct internal research to improve, repaid, or develop products, services, or technology;
- Identify and repair technical errors that impair existing or intended functionality;

- Perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller;
- Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;
- Protect the vital interests of the consumer or of another individual;
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action;
- Process personal data for certain reasons of public interest;

❖ The obligations do not apply where compliance by the controller or processor would violate an evidentiary privilege under Colorado Law.

❖ The obligations will not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Colorado Law as part of a privileged communications.

❖ The obligations do not apply where they would adversely affect the rights or freedoms of any persons.

❖ The obligations do not apply to the processing of personal data by an individual in the course of a purely personal or household activity.

Vendor Provisions

❖ A controller or processor that discloses personal data to another controller or processor in compliance with the Act does not violate the Act if the recipient processes the personal data in violation of the Act and, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

- A controller or processor receiving personal data from a controller or processor in compliance with the Act does not violate the Act if the controller or processor from which it receives the personal data fails to comply with applicable obligations.

- A processor shall adhere to the instruction of the controller and assist the controller to meet its obligations under the Act.

- Processing by a processor must be governed by a binding contract between the controller and the processor that sets out the processing instructions to which the processor is bound.

Connecticut

An Act Concerning Consumer Privacy

- Link to Text: SB 893
- Effective Date: January 1, 2023
- Status: Referred by Senate to Committee on Judiciary

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children[6]	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is a Connecticut resident acting only in an individual or household context.
- ***Consumer*** does not include a natural person acting in a commercial or employment context.
- ***Controller*** means the natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- ***Personal Data*** means any information that is linked or reasonably linkable to an identified or identifiable natural person.
- ***Personal Data*** does not include de-identified data or publicly available information.

[6] Compliance with COPPA is compliance with this act in regard to parental consent requirements.

Enforcement

- The Attorney General may bring action seeking injunctive relief, up to $7,500 civil penalties for each violation in the name of the state, or on behalf of persons residing in the state.

- The Attorney General must provide the controller or processor written notice specifying the alleged violations. If the controller or processor cures and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action for statutory damages shall be initiated against the controller or processor.

- There is no ***Private Right of Action.***

Data Safe Harbors

- This act applies to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that:

  - Control or process personal data of not less than 100,000 consumers; or

  - Control or process personal data of not less than 25,000 consumers and that derive more than 50% of their gross revenue from the sale of personal data

- A controller or processor need not comply with an authenticated consumer rights request if the controller:

  - Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

  - Does not use the personal data to recognize or respond to the specific customer who is the subject of the personal data; and

  - Does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in Section 8.

- This act does not apply to
  - State government entities;
  - Financial institutions or data governed by the Gramm-Leach-Bliley Act;
  - Covered entities or associates governed under HIPAA, and the Health Information Technology for Economic and Clinical Health Act;
  - Nonprofit organizations;
  - Institutions of higher learning.
- Data exemptions include information that meets the definition of:
  - Protected Health Information under HIPAA
  - Health records
  - Patient identifying information for purposes of 42 U.S.C. 290dd-2
  - Identifiable private information for purposes of the Federal Policy for Protection of Human Subjects under 45 CFR 46
  - Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use
  - The protection of human subjects under 21 CFR 6, 50 and 56 or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law
  - Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.
  - Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq.

- HIPAA de-identified information
- Information that is derived from any health care information listed above that has been de-identified in accordance with HIPAA
- Information originating from, and intermingled to be indistinguishable with any of the health care-related information listed above that is maintained by:
    - A covered entity or business associate as defined by HIPAA; or
    - A program or a qualified service organization as defined by 42 USC 290dd-2
- Information used only for public health activities and purposes as described in HIPAA

- An activity involving the collection, maintenance, disclosure, sale, communication or use of any personal data bearing on a consumer's credit worthiness, credit capacity, character, general reputation, personal characteristics or mode of living pursuant to the Fair Credit Reporting Act — to the extent that such activity is regulated and authorized by that act
- Data collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994 or the federal Farm Credit Act, 12 USC 2001 et seq.
- Personal data regulated by the Family Educations Rights and Privacy Act
- Information maintained for emergency contact, job applicant, employment records, or benefit administration purposes
- This act does not restrict a controller or processor's ability to
    - Comply with federal, state or municipal ordinances or regulations;
    - Comply with civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state or governmental authorities

- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or local laws, rules or regulations
- Investigate, establish, exercise, prepare for or defend legal claims
- Complete the transaction for which the information was collected;
- Provide a good or service requested by the consumer;
- Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;
- Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;
- Conduct internal research to develop, improve, or repair products, services or technology;
- Effectuate a product recall;
- Comply with an evidentiary privilege
- Identify and repair technical errors that impair existing intended functionality;
- Exercise free speech
- Prevent, detect, and protect against or respond to a security incident; identify theft, fraud, harassment, malicious, deceptive, or illegal activity; preserve the integrity or security systems or to investigate, report, or prosecute those responsible for such illegal activity;
- To perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product

or service specifically requested by a consumer or the performance of a contract to which the consumer is a party;

- Assist another controller, processor, or third party with any of the obligations under sections 1 to 8, inclusive, of this act, this section and sections 10 and 11 of this act; or

- Engage in public or peer-reviewed scientific, or statistical research that is in the public interest and that adheres to all other applicable ethics and privacy laws, and is monitored and governed by an institutional review board, or similar independent oversight entities that determine:

    - If deletion is likely to provide substantial benefits that do not exclusively accrue to the controller;

    - The expected benefits of the research outweigh the privacy risks; and

    - If the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

❖ See full list at link provided above.

Vendor Provisions

❖ Processing by a processor is governed by the contract between the controller and the processor. The contract shall include requirements that the processor shall:

o Ensure that each person processing the data is subject to a duty of confidentiality with respect to the data;

o At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of data is required by law;

o Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations of sections 1 to 11; and

- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 1 to 11, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon written request.

❖ A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations pursuant to sections 1 to 11. Assistance includes:

- Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measure, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

- Taking into account the nature of processing the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor, in order to meet the controller's obligations; and

- Providing necessary information to enable the controller to conduct and document data protection assessments.

❖ A controller or processor that discloses to a third party controller or processor is not liable for a violation by the receiving party unless the disclosing party had actual knowledge that the service provider intended to violate this act.

Florida

Consumer Data Privacy

- Legislative Status: Passed by Senate, In House 04/29/2021; Effective July 1, 2022
- Link to Text: HB 969

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓
Opt in	✓	

Key Definitions

- ***Consumer*** means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, who is acting in a personal capacity or household context. The term does not include a natural person acting on behalf of a legal entity in a commercial or employment context.

- ***Controller*** means either:

  (1) A for-profit legal entity that:

  - Does business in this state;
  - Collects personal information about consumers, or is the entity on behalf of which such information is collected;
  - Determines the purposes and means of processing personal information about consumers alone or jointly with others; and

- Satisfies at least two of the following thresholds:
    - (I) Has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.
    - (II) Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices for targeted advertising in conjunction with third parties or that is not covered by an exception under this section.
    - (III) Derives 50% or more of its global annual revenues from selling or sharing personal information about consumers; or

(2) Any entity that controls or is controlled by a controller.

❖ ***Personal information*** means information that identifies, relates to, or describes a consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a consumer or household. The term includes, but is not limited to, the following:

- Identifiers such as a real name, alias, postal address, unique identifier, online identifier, internet protocol address, email address, account name, Social Security number, driver license number, passport number, or other similar identifiers.
- Information that identifies, relates to, or describes, or could be associated with, a particular individual, including, but not limited to, a name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
- Characteristics of protected classifications under state or federal law.

- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

- Biometric information.

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

- Geolocation data.

- Audio, electronic, visual, thermal, olfactory, or similar information.

- Inferences drawn from any of the information identified in this paragraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

o ***Personal information*** does *not* include consumer information that is:

- Consumer employment contact information, which includes a position name or title, employment qualifications, emergency contact information, business telephone number, business address, business electronic mail address, business facsimile number, employee benefit information, and similar information used solely in an employment context.

- de-identified or aggregate consumer information.

- Publicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions:

    - From federal, state, or local government records.
    - By a widely distributed media source.
    - By the consumer or by someone to whom the consumer disclosed the information unless the consumer has purposely and effectively restricted the information to a certain audience on a private account.

- ***Processor*** means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a controller and to which the controller discloses a consumer's personal information pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the controller, or as otherwise permitted by this section.

Enforcement

- ***Private Right of Action***
  - A Florida consumer may bring a civil action against a controller, processor, or person pursuant to this section for certain violations.
- ***Department Enforcement***
  - A violation of this section is an unfair and deceptive trade practice, actionable by the Department of Legal Affairs.

Data Safe Harbors

- This section does not restrict the ability of any controller, processor, or third party to do any of the following:
  - Collect and transmit personal information that is necessary for the sole purpose of sharing such personal information with a financial service provider to facilitate short term, transactional payment processing for the purchase of products or services.
  - Comply with federal, state, or local laws.
  - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

- Cooperate with law enforcement agencies concerning conduct or activity that the controller, processor, or third party reasonably and in good faith believes may violate federal, state, or local law.

- Exercise legal rights or privileges.

- Collect, use, retain, sell, share, or disclose de-identified personal information or aggregate consumer information.

❖ This section does not apply to:

- Personal information used or collected by a controller or processor pursuant to a written contract between the controller and processor that complies with the requirements of this section. Such information cannot be sold, shared, or disclosed to another person unless otherwise authorized under this section.

- Personal information used by a controller or processor to advertise or market products or services that are produced or offered directly by the controller or processor. Such information may not be sold, shared, or disclosed to another person unless otherwise authorized under this section.

- Personal information collected by a controller of a natural person acting in the role of a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of the controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller.

- Protected health information under HIPAA and patient identifying information under 42 C.F.R. Part 2.

- Health information collected by a covered entity or business associate.

- Information collected as part of a clinical trial subject to the Federal Policy For The Protection Of Human Subjects.

- Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26.

- Information used only for public health activities and purposes as described in 45 C.F.R. s. 164.512.

- Personal information collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act.

- Information collected as part of a clinical trial subject to the Federal Policy For The Protection Of Human Subjects.

- Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. s. 2721 et. seq. 14. Education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.

- Information collected as part of public or peer-reviewed scientific or statistical research in the public interest.

Vendor Provisions

- A controller that collects a consumer's personal information shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure. A controller must require any processors to implement and maintain the same or similar security procedures and practices for personal information.

Florida

Florida Privacy Protection Act

- Legislative Status: Died in Senate 04/28/2021
- Link to Text: SB 1734

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓
Opt in	✓	

Key Definitions

- ***Business*** means either:
  - A for-profit legal entity that meets the following requirements:
    - Does business in this state;
    - Collects personal information about consumers, or is the entity on behalf of which such information is collected;
    - Determines the purposes and means of processing personal information about consumers, alone or jointly with others; and
    - Satisfies either of the following thresholds:

- Annually buys, sells, or shares the personal information of 100,000 or more consumers, households, or devices.
- Derives 50% or more of its global annual revenues from selling or sharing personal information about consumers; or

➢ An entity that controls or is controlled by a business and that shares common branding with the business.

❖ ***Consumer*** means a natural person, however identified, including identification by a unique identifier, who is in this state for other than a temporary or transitory purpose. The term does not include any other natural person who is a nonresident.

❖ ***Personal Information*** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The term includes, but is not limited to, all of the following items of personal identifying information about a consumer collected and maintained by a person or business:

➢ A first and last name.

➢ A home or other physical address that includes the name of a street and the name of a city or town.

➢ An electronic mail address.

➢ A telephone number.

➢ A Social Security number.

➢ An identifier such as an alias, a unique personal identifier, an online identifier, an Internet Protocol address, an account name, a drivers license number, a passport number, or other similar identifiers.

➢ Biometric information, such as DNA or fingerprints or any other biometric information collected by a business about a consumer without the consumer's knowledge.

- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with a website, an application, or an advertisement.

- Audio, electronic, visual, thermal, olfactory, geolocation, or similar information.

- Professional or employment-related information.

- Education information, defined as only information that is not publicly available.

- Inferences drawn from any information specified in this paragraph which can create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

- Any other information that may serve as a probabilistic identifier concerning a consumer which is collected from the consumer through a website, an online service, or some other means by the business and maintained by the business in combination with an identifier in a form that, when used together with the information, identifies the consumer.

- Characteristics of protected classifications under state or federal law.

- Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies.

- Geolocation data.

❖ ***Service Provider*** means a person who processes personal information on behalf of a business to whom the business discloses a consumer's personal information for a business purpose pursuant to a written or electronic contract if the contract prohibits the person from:

  - Selling the information;

  - Retaining, using, or disclosing the personal information for any purpose other than the business purposes specified in the contract, including a prohibition on

retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business;

- Combining the personal information that the service provider receives from or on behalf of the business with personal information that the service provider receives from or on behalf of another person or persons or collects from its own interaction with consumers, provided that the service provider may combine personal information to perform a business purpose; and

- Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

Enforcement

- ***Department of Legal Affairs***

  - The Department of Legal Affairs may adopt rules to implement this section.

- ***No Private Right of Action***

Data Safe Harbors

- Personal Information does not include:

  - Information about a consumer obtained from public records, including information that is lawfully made available from federal, state, or local governmental records; information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or lawfully obtained, truthful information that is a matter of public concern.

  - Consumer information that is de-identified or aggregate consumer information that relates to a group or category of consumers from which individual consumer identities have been removed.

Vendor Provisions

- A business that collects a consumer's personal information and discloses it to a service provider for a business purpose shall enter into an agreement with such service provider that obligates the service provider to comply with applicable obligations under this Act and to provide the same level of privacy protection as is required by this act.

- If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, the provider or person must notify the business of that engagement, and the engagement must be pursuant to a written contract that includes the prohibitions described in s. 501.174(24) and a certification made by the person receiving the personal information that he or she understands the restrictions under this act and will comply with them.

Hawaii

Relating to Privacy

- Legislative Status: died in committee
- Link to Text: SB 418

Hawaii's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction	✓	

Key Definitions

- ***Consumer*** means an individual who interacts with a business within the state.

- ***Identifying Information*** means information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked with a particular consumer or household, including:

  - Name, alias, postal address, unique identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number or passport number, signature, Biometric information

  - Protected classifications

  - Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming history or tendencies

  - Biometric information

- Internet and other electronic network activity information including browsing history, search history and information regarding a consumer's interaction with an internet web site, application or advertisement
- Geolocation data
- Audio, electronic, visual or similar recordings Professional or employment-related information
- Education records
- Medical data
- Insurance information
- Financial information
- Profiles about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes or intelligence created from inferences from any other information collected from a consumer

❖ Hawaii's law does not define ***Business***.

Enforcement

❖ This law shall be enforced by the office consumer protection.

❖ There is no ***Private Right of Action***

There are no ***Data Safe Harbors***

There are no ***Vendor Provisions***

Hawaii

Relating to Privacy

- Legislative Status: Deferred by Committee on JDC
- Link to Text: HB 2572

Hawaii's Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction	✓	

Key Definitions

- ***Consumer*** means an individual residing in the state.

- ***Personal Information*** means an identifier in combination with one or more specified data elements, when the specified data element or elements are not encrypted or otherwise rendered unreadable. Personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

- ***Identifier*** means a common piece of information related specifically to an individual, that is commonly used to identify that individual across technology platforms, including a first name or initial, and last name; a user name for an online account; a phone number; or an email address.

- ***Specified Data Element*** means any of the following:

  - An individual's Social Security number, either in its entirety or the last four or more digits

- Driver's license number, federal or state identification card number, or passport number
- A federal individual taxpayer identification number
- An individual's financial account number or credit or debit card number
- A security code, access code, personal identification number or password that would allow access to an individual's account
- Health insurance policy number, subscriber identification number or any other unique number used by a health insurer to identify a person
- Medical history, medical treatment by a health-care professional, diagnosis of mental or physical condition by a health care professional or deoxyribonucleic acid profile
- Unique biometric data generated from a measurement or analysis of human body characteristics used for authentication purposes, such as fingerprint, voice print, retina or iris image, or other unique physical or digital representation of biometric data; and
- A private key that is unique to an individual and that is used to authenticate or sign an electronic record

❖ ***Business Purpose*** means the use of personal information for a business's operational purposes, or other notified purposes; provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

❖ ***Collect(ed)(ion)*** means buying, renting, gathering, obtaining, receiving or accessing any personal information pertaining to a consumer by any means, including receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

Enforcement

- A business that violates any provision shall be subject to a fine of $7,500 for each offense.
- Attorney General may adopt rules pursuant to Chapter 91 to implement provisions of this section and conduct civil investigations.

Data Safe Harbor Provisions

- Contact tracing information that is recorded/collected without the consent of the individual who is the primary user of the device or application
- Geolocation information to detect security incidents

Vendor Provisions

- Third-party data brokers buying and reselling people's information and data are required to register with the state.

Illinois

Data Transparency and Privacy Act

- Legislative Status: In Senate
- Link to Text: HB 3358

Consumer Rights	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** is defined as a resident of Illinois who provides personal information to a private entity in the course of purchasing, viewing, accessing, renting, leasing or otherwise using real or personal property, or any interest therein, or obtaining a product or service from the private entity, including advertising or any other content.

  Consumer does not include a person from whom personal information is collected while that person is acting in an employment context.

- ***Personal Information*** is defined as any information that is linked, or can reasonably be linked, to a particular consumer, including name, alias, signature, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit card number, debit card number or any other financial account information, unique personal identifier, geolocation or biometric information.

- ***Business*** is defined as a for-profit legal entity that does business in the state of Illinois, and satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million
- Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or
- Derives 50% or more of its annual revenues from selling consumers' personal information

Enforcement

- The Attorney General has exclusive authority to enforce this act.
- There is no ***Private Right of Action***

Data Safe Harbors

- Disclosure of personal information by a private entity under a written contract authorizing the third party to utilize the personal information for limited purposes of performing services on behalf of the private entity
- Disclosure of personal information based on a good faith belief that disclosure is required to comply with applicable law, regulation, legal process or court order; or
- Disclosure of personal information by a private entity to address fraud, security or technical issues, to protect the disclosing private entity's rights or property, or to protect consumers or public from illegal activities;
- Health care provider or other covered entity subject to HIPAA;
- Financial institution or subject to GLBA; and
- To a contractor, subcontractor or agent of a state agency or local unit of government when working for that state agency or local unit of government;
- See full list at link provided above.

Vendor Provisions

- If a third party materially alters how it uses or shares personal information in a manner that is inconsistent with the promises made at the time of collection, it shall provide prior notice of the changed practice to the consumer.

Illinois

Consumer Privacy Act

- Legislative Status: Referred to Rules Committee 03/27/21
- Link to Text: HB 3910

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Business*** means a for-profit legal entity that collects consumers' personal information, or on behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in this state, and that satisfies one or more of the following thresholds:
  - Has annual gross revenues in excess of $25 million, as adjusted in accordance with paragraph (5) of subsection (a) of Section 80.
  - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
  - Derives 50% or more of its annual revenues from selling consumers' personal information. (2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business.

- ***Personal Information*** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. "Personal information" includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

  - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.

  - Any personal information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

  - Characteristics of protected classifications under state or federal law.

  - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

  - Biometric information.

  - Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

  - Geolocation data.

  - Audio, electronic, visual, thermal, olfactory, or similar information.

- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99).
- Inferences drawn from any of the information identified in this subsection to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

"Personal information" does not include publicly available information.

Service Provider means a for-profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose in accordance with a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this Act, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

Enforcement

- ***Attorney General***
  - The Attorney General may enforce the Act.
- ***Private Right of Action***
  - Any consumer whose unencrypted or un-redacted personal information, as defined in Section 5 of the Personal Information Protection Act, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.

Data Safe Harbors

- A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:
  - Complete the transaction for which the personal information was collected; provide a good or service requested by the consumer or reasonably anticipated within the context of a business's ongoing business relationship with the consumer; or otherwise perform a contract between the business and the consumer.
  - Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
  - Debug to identify and repair errors that impair existing intended functionality.
  - Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
  - Comply with the Citizen Privacy Protection Act.
  - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
  - Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
  - Comply with a legal obligation.
  - Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Vendor Provisions

- A business that discloses personal information to a service provider shall not be liable under this Act if the service provider receiving the personal information uses it in violation of the restrictions set forth in this Act, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation.

- A service provider shall likewise not be liable under this Act if a third party materially alters how it uses or shares personal information in a manner that is inconsistent with the promises made at the time of collection. It shall provide prior notice of the changed practice to the consumer services as set forth in this Act.

Illinois

Data Transparency and Privacy Act

- Legislative Status: Referred to Assignments; 4/12/2020
- Link to Text: SB 2330

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Business*** means any sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that does business in the state of Illinois and meets one or more of the following thresholds:
  - The business collects or discloses the personal information of 50,000 or more persons, Illinois households or the combination thereof; or
  - Derives 50% or more of its annual revenues from selling consumers' personal information
- ***Business*** does *not* include any third party that operates, hosts or manages, but does not own a website or online service on the owner's behalf or by processing information on behalf of the owners, or any state and local governments or municipal corporations.
- ***Consumer*** means a natural person residing this state. Consumer does ***NOT*** include a natural person acting in an employment context.

- ***Personal Information*** means information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:
  - Identifiers such as a real name, alias, signature, postal address, telephone number, unique personal identifier, email address, account name, SSN, driver's license number, state identification number, passport number, physical characteristics or description, insurance policy number, employment, employment history, bank account number, credit card number, debit card number, financial information, medical information, health insurance information or other similar identifiers

Enforcement

- The Attorney General has authority to enforce this act as a violation of the Consumer Fraud and Deceptive Business Practices Act.
- ***Private Right of Action***
  - A consumer may bring civil suit for any of the following:
    - To recover damages in an amount not less than $100 and not greater than $750 per customer per incident or actual damages, whichever is greater
    - Injunctive or declaratory relief
    - Any other relief the court deems proper

Data Safe Harbors

- This act does not apply to personal information collected, processed, sold or disclosed under:
  - The GLBA
  - HIPAA
  - The Fair Credit Reporting Act

- Collect or disclose a consumer's personal information if a consumer's conduct takes place wholly outside of Illinois

Vendor Provision

- Affiliates and third parties shall not sell consumer personal information purchased from a business unless the consumer has received notice and is provided an opportunity to opt out of the resale of the consumer's personal info.

Illinois

Data Privacy Act

- Legislative Status: In Senate
- Link to Text: SB 2263

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out		✓
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is an Illinois resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

- ***Controller*** means a natural or legal person, which alone or jointly with others, determines the purposes and means of the processing of personal data.

- ***Personal data*** means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include de-identified data or publicly available information.

- ***Sensitive data*** means (a) personal data revealing racial/ethnic origin, religious beliefs, mental or physical health condition or diagnosis, or sex life or sexual orientation; (b) processing of genetic or biometric data (c) personal data of a child.

Enforcement Provisions

- The Attorney General may bring an action on behalf of the state, or as parens patriae on behalf of persons residing in the state, to enforce this act.
- Any controller or processor that violates this act is subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.
- There is no ***Private Right of Action***

Data Safe Harbor Provisions

- State and local governments
- Municipal corporations
- Information that meets the definition of
  - Protected Health Information for purposes of HIPAA
  - Patient identifying information for purposes of 42 C.F.R. Part 2
  - Identifiable private information for purposes of the federal policy for the protection of human subjects
  - Information and documents created by a quality improvement committee of a health care facility
  - Patient safety work product information
- Personal data provided to, from or held by a consumer reporting agency
- Personal data collected, processed, sold or disclosed pursuant to the GLBA
- Personal data collected, processed, sold or disclosed pursuant to the federal Driver's Privacy Protection Act

- Data maintained for employment records purposes
- See full list at link provided above

Vendor Provisions

- Third parties must honor objection requests received from third-party controllers.

Illinois

Consumer Privacy Act

- Legislative Status: In Senate
- Link to Text: HB 5603

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Business*** means any legal entity organized or operated for the profit or financial benefit of its shareholders, that collects consumers' personal information, or on behalf of which such information is collected and that alone or jointly with others determines the purposes and means of the processing of consumers' personal information. Satisfies one OR more of the following thresholds:
  - Annual gross revenue exceeds $25 million
  - Annually buys, receives for the business's purpose, sells, or shares for commercial purpose, personal information of 50,000 or more consumers, households, or devices
  - Derives 50% or more of annual revenues from selling consumers personal info
- ***Consumer*** means a natural person who is an Illinois resident.

- ***Personal Information*** means any information that identifies or is related to in any way identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number or other similar identifiers.

Enforcement Provisions

- The Attorney General may bring an action seeking an injunction and a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

- There is no ***Private Right of Action***

Data Safe Harbor Provisions

- Comply with federal, state or local laws

- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state or local authorities

- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state or local law

- Exercise or defend legal claims

- Collect, use, retain, sell or disclose consumer information that is de-identified or in the aggregate consumer information

- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of Illinois

- A provider of health care or medical information protected from disclosure under state confidentiality laws on patient health information or Protected Health Information that is collected by a covered entity or business associate governed by the privacy, security and breach notification rules established by HIPAA

- Information collected as part of a clinical trial subject to the Federal Policy for the protection of Human Subjects

- See full list at link provided above

Vendor Provisions

- A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice.

Kentucky

An act relating to consumer privacy of personal information

- Legislative Status: Died in Committee
- Link to Text: HB 408

Consumer Rights	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Opt In		✓
Children[7]	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a person who seeks or acquires, by purchase or lease, any good, service, money, or credit for personal, family, or household purposes.

- ***Personal Information*** means the same thing as "personally identifiable information" in KRS 365.720(4) and also includes geolocation data. KRS 365.720(4): "Personally identifiable information" means data capable of being associated with a particular customer through one (1) or more identifiers, including but not limited to a customer's name, address, telephone number, electronic mail address, fingerprints, photographs or computerized image, Social Security number, passport number, driver identification number, personal identification card number or code, date of birth, medical information, financial information, tax information, and disability information.

[7] The right to opt in if younger than 16, and the minor can opt in if older than 13.

- ***Business*** means a sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for commercial purposes that:
  - Satisfies one (1) or more of the following:
    - Has annual gross revenues in excess of $25 million dollars;
    - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or
    - Derives 50% or more of its annual revenues from selling consumers' personal information;
  - Collects and maintains personal information from consumers who reside in Kentucky or use or visit the internet web site or online service; and
  - Purposefully directs its activities toward Kentucky, consummates some transaction with Kentucky or a resident thereof, purposefully avails itself of the privilege of conducting activities in Kentucky, or otherwise engages in any activity that constitutes sufficient nexus with Kentucky to satisfy the requirements of the United States Constitution.
- ***Business*** does <u>not</u> include:
  - A third party that operates, hosts, or manages an internet website or online service on behalf of its owner or processes information on behalf of the owner of an internet website or online service;
  - A financial institution or affiliate of a financial institution that is subject to the Gramm-Leach-Bliley Act or the Fair Credit Reporting Act;
  - An entity subject to HIPAA;
  - A manufacturer of a motor vehicle or a person who repairs or services a motor vehicle who collects, generates, records, or stores covered information that is:

- Retrieved from a motor vehicle in connection with a technology or service related to the motor vehicle; or

- Provided by a consumer in connection with a subscription or registration for a technology or service related to the motor vehicle.

Enforcement

- After the business has been given notice of the alleged violations and failed to cure for 30 days, the Attorney General may enforce this act by instituting an appropriate legal proceeding against the business seeking an injunction and civil penalties not greater than $5,000 per violation.

- This act nowhere mentions a ***Private Right of Action.***

Data Safe Harbors

- This act does not apply to (1) nonprofits; (2) governmental entities; (3) entities under HIPAA, the Fair Credit Reporting Act; or Gramm-Leach-Bliley; or (4) certain entities that manufacture, repair, or service motor vehicles.

Vendor Provisions

- This act does not create specific vendor provisions.

Maine

Broadband Internet Access Service Customer Privacy

- Legislative Status: Enacted
- Effective Date: 7/1/2020
- Link to Text: ME SB 275 (LD 946)

Maine Consumer Rights Checklist	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt In	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Customer*** is defined as applicant for or a current or former subscriber of broadband Internet access service.

- ***Personal Information*** is defined as personally identifying information about a customer, including name, billing information, Social Security number, billing address and demographic data; and information form a customer's use of broadband internet access service including web browsing history, usage history, precise geolocation information, financial information, health information, information pertaining to the customer's children, the origin and destination internet protocol address or the content of the customer's communications the customer's device identifier, such as a media access control address, international mobile equipment identity or Internet protocol address.

- ***Provider*** is defined as a person or provider who provides broadband internet access service within the state to customers physically located and billed for service received in the state.

Enforcement

- There is no ***Enforcement*** provision
- There is no ***Private Right of Action***

Data Safe Harbors

- Information obtained for the purpose of providing the service from which such information is derived or for the services necessary to the provision of such service
- To advertise or market the provider's communications-related services to the customer
- To comply with a lawful court order
- To initiate, render, bill for and collect payment for broadband internet access service
- To protect users of the provider's or other providers' services from fraudulent, abusive or unlawful use of or subscription to such services
- To provide geolocation information concerning the customer to respond to emergency services

There are no ***Vendor Provisions***

Maryland

Online Consumer Protection Act

- Legislative Status: Died in Committee
- Effective Date:
- Link to Text: SB 613

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means any individual who resides in Maryland.

- ***Personal Information*** means any information relating to an identified or identifiable consumer and information that identifies relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device.

  Personal Information does not include:

  - Information that is lawfully made available from federal, state or local government records

  - Consumer information that is de-identified or aggregate consumer information

- ***Business*** means any for-profit legal entity that collects the personal information of state consumers; and satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $25 million
- Annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households or devices; or
- Derives at least half of its annual revenues from selling consumers' personal information

- A ***Business*** may also be defined as an entity that controls or is controlled by a business as defined above and shares a name, service mark or trademark with the business.

Enforcement

- When the Office of the Attorney General has a reason to believe that the act has been violated, the Attorney General may bring an action to restrain the violation by temporary restraining order or preliminary or permanent injunction and seek a civil penalty not exceeding $2,500 for each violation or not exceeding $7,500 for each intentional violation.

- There is no ***Private Right of Action***

Data Safe Harbors

- A business collecting or disclosing personal information of the business's employees if the business is collecting or disclosing the information within the scope of its role as an employer

- Health information collected by a covered entity or business associate

- A Covered Entity governed by the privacy, security, and breach notification rules established in accordance with HIPAA

- Information collected as part of a clinical trial subject to the Federal Policy For The Protection Of Human Subjects

- Sale of personal information to or from a consumer reporting agency if that information is to be used to generate a consumer report

- Personal information processed under the GLBA
- Personal information processed under the Federal Driver's Privacy Protection Act of 1994
- Education information covered by the Federal Family Educational Rights and Privacy Act

There are no ***Vendor Provisions***

Maryland

Consumer Privacy and Data Collection

- Legislative Status: Died in Committee
- Link to Text: HB 1656

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means an individual who resides in the state.

- ***Business*** means any legal entity that is: (1) organized for profit (2) collects personal information of an individual or consumer, ***AND*** (3) satisfies one or more of the following thresholds:

  - Annual gross revenues in excess of $25 million

  - Annually buys, receives for the business's commercial purpose, sells, or shares for commercial purposes, alone or in combination the personal information of 50,000 or more consumers, households, or devices; or

  - Derives at least half of its annual revenues from selling consumers' personal information

- ***Personal Information*** means information that identifies or relates to identifiers such a real name, an alias, a postal address, a unique personal identifier, an online identifier, an

internet protocol address, an e-mail address, an account name, a SSN, a driver's license number, a passport number or other information that identifies, relates to, describes, or is capable of being associated with a particular individual.

Enforcement

- The Attorney General may bring an action for an injunction and a civil penalty.
- A person who intentionally violates this act is subject to a civil penalty not exceeding $7,500 for each violation.
- There is no ***Private Right of Action***

Data Safe Harbors

- Comply with federal, state, or local laws
- Comply with a civil, criminal or regular inquiry, investigation, subpoena or summons by a federal, state or local authority
- Cooperate with a law enforcement agency concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law
- Exercise legal rights or privileges
- Collect, use, retain, sell, or disclose consumer information that is de-identified or consumer information in the aggregate
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of the state, provided that if the business collected the information while the consumer was outside the state:
  - No part of the sale of the consumer's personal information occurred in the state; and
  - No personal information collected while the consumer was in the state is sold

- A business collecting or disclosing personal information of the business's employees to the extent that the business is collecting or disclosing the information within the scope of its role as an employer

- Medical or health information that is collected by a covered entity or business associate governed by state law or the privacy, security and breach notification rules established by HIPAA

- The sale of personal information to or from a consumer reporting agency of that information is to be reported in or used to generate a consumer report

- Personal information collected, processed, sold, or disclosed under the GLBA

- Personal information collected, processed, sold or disclosed under the federal Driver's Privacy Protection Act

There are no ***Vendor Provisions***

Maryland

Online Consumer Protection Act

- Legislative Status: Introduced February 10, 2021
- Link to Text: SB 0930

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Business*** means a for-profit legal entity that collects the personal information of an individual or consumer satisfies one or more of the following thresholds:
  - Has annual gross revenues in excess of $25 million;
  - Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or
  - Derives at least half of its annual revenues from selling consumers' personal information; or any entity that: (i) controls or is controlled by a business under item (1) of this subsection; and (ii) shares a name, service mark, or trademark with the business.
- ***Consumer*** means an individual who resides in the state.

- ***Personal Information*** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device.
    - Personal Information does not include: (i) publicly available information that is lawfully made available from federal, state, or local government records; (ii) de–identified consumer information; or (iii) aggregate consumer information.
- ***Service Provider*** means a person that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose in accordance with a written contract if the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise allowed by this subtitle.

Enforcement

- ***Attorney General***
    - A violation of this subtitle is an unfair, abusive, or deceptive trade practice.
    - The Attorney General may adopt regulations to carry out the Act.
- ***Private Right of Action***
    - No private right of action.

Data Safe Harbors

- A business or service provider is not required to comply with a consumer's request to delete their personal information if it is necessary to maintain the personal information in order to:
    - Complete the transaction for which the personal information was collected;
    - Perform a contract with the consumer;

- Detect security incidents;
- Protect against malicious, fraudulent or illegal activity or prosecute those responsible for those activities;
- Identify or repair errors that impair existing intended functionality;
- Exercise free speech;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, in some circumstances; or
- Comply with legal obligations.

❖ The obligations don't restrict a business or third party from:

- Complying with federal, state or local laws;
- Complying with a civil, criminal or regulatory inquiry;
- Cooperating with a law enforcement agency concerning conduct or activity that violate federal, state, or local law;
- Exercising legal rights or privileges;
- Engaging in news-gathering activities protected by the First Amendment.

❖ Additional Safe Harbors:

- A business collecting or disclosing personal information of the business's employees if the business is collecting or disclosing the information within the scope of its role as an employer
- Health information collected by a covered entity or business associate
- A covered entity governed by the privacy, security, and breach notification rules established in accordance with HIPAA

- Information collected as part of a clinical trial subject to the Federal Policy For The Protection Of Human Subjects

- Sale of personal information to or from a consumer reporting agency if that information is to be used to generate a consumer report

- Personal information processed under the GLBA

- Personal information processed under the Federal Driver's Privacy Protection Act of 1994

There are no ***Vendor Provisions***

Massachusetts

The Massachusetts Information Privacy Act

- Link to Text: SD 1726 (substantively identical to HD 2664)
- Effective Date: 12 months after enacted (§ 2 effective immediately)
- Legislative Status: Referred to Joint Committee on Public Service

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Annual Opt In	✓	
Children[8]	✓	
Data Destruction[9]	✓	
Right to not be Surreptitiously Surveilled[10]	✓	

Key Definitions

- ***Consent*** means freely given, specific, informed, and unambiguous opt-in consent by an individual.

- ***Individual*** means a natural person who is a Commonwealth of Massachusetts resident. Location within the commonwealth creates a presumption of residency.

- ***Personal Information*** means (1) information about an individual directly or indirectly captured in a covered interaction; and (2) any information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device. Information is reasonably linkable to an individual, household, or device if it can be used on its own or in combination with other reasonably available information to identify an individual,

[8] Children 13 and older can exercise rights.
[9] Biometric and location information must be destroyed after consent expires.
[10] Also rights restricting employers surveilling employees.

household, or device regardless of whether the covered entity holds such information. Please see the text link above for a full list.

- ***Biometric Information*** means information that pertains to measurable biological or behavioral characteristics that can be used along or in combination with each other or with other information for automated recognition of a known or unknown individual.

- ***Biometric Information*** does not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, physical descriptions (such as height, weight, hair color, or eye color), certain donated organs (including tissue, parts, blood, or serum), health information covered under HIPAA, or scans used to diagnose or treat medical conditions or validate scientific tests.

- ***Covered Entity*** means an entity that conducts business in the Commonwealth of Massachusetts, processes personal information by itself or by contracting with a data processor, and:

  - Has earned or received $10 million or more of annual revenue through 300 or more transactions; or

  - Processes or maintains the captured personal information of more than 10,000 unique individuals during the course of a calendar year.

- ***Entity*** does not include a Massachusetts governmental entity.

- ***Massachusetts governmental entity*** means any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose.

- ***Processing*** means any action or set of actions performed on or with personal information.

  - This includes collecting, sharing, accessing, using, storing, transmitting, etc.

  - This also includes destroying and de-identifying.

- **Harm** means "potential or realized adverse consequences to an individual or society . . ."
  - Please see text above for full list.

Enforcement

- The Attorney General may bring an action against a covered entity, data processor, or third party to remedy violations. If the defendant knew or should have known that its method, act, or practice would violate this chapter, then the court may impose a civil penalty equal to the range of administrative penalties available below.
- This chapter is also enforced by the Massachusetts Information Privacy Commission established by section 79 of chapter 10.
- No private or government action brought pursuant to this chapter shall preclude any other action under this chapter.
- ***Administrative Penalties***
  - Not less than or $15,000 or 0.15% of the covered entity, data processor, or third party's annual global revenue per individual violation (whichever is greater); and
  - Not more than $20 million per violation or 4% of the covered entity, data processor, or third party's annual global revenue (whichever is greater).
  - The accused entity has a right to an adjudicatory hearing, and the chapter alludes to the possibility of consent decrees.
- ***Private Right of Action***
  - An individual or group of individuals alleging a violation of this chapter or a regulation promulgated under this chapter may bring an administrative complaint before the Commission.
  - Any individual alleging a violation of this chapter or a regulation promulgated under this chapter may bring a civil action in any court of competent jurisdiction seeking liquidated damages not less than 0.15% of the annual global revenue of the covered entity or $15,000 per violation (whichever is greater); punitive

damages; reasonable attorney's fees and costs; and equitable remedies including injunctions.

- A violation of this chapter or a regulation promulgated under this chapter regarding an individual's personal information creates a rebuttable presumption of harm to that individual.

- An individual cannot be required to file an administrative complaint.

Data Safe Harbors

- Aspects of the bill do not apply to Massachusetts governmental entities, but a governmental entity can be a third party.

- No covered entity that is a provider of interactive computer service under 47 U.S.C. § 230 shall be treated as the publisher or speaker of any personal information provided by another information content provider, as defined in 47 U.S.C. § 230 and allowing posting of information by a user without other action by the interactive computer service shall not be deemed processing of the personal information by the interactive computer service.

- Nothing in this chapter shall diminish any individual's rights or obligations under the Massachusetts Fair Information Practices Act and its regulations.

- A covered entity may provide discounts based on an individual's prior purchases, provided the persona information shall be processed solely for operating the program, without violating the provision against discount programs that are tied to the consumer's degree of acceptance of personal information processing.

- The bill does not apply to:

  - Individuals sharing their personal contact information with other individuals in the workplace, social, political or similar settings where the purpose of the information is to facilitate communication among such individuals; however, processing this information beyond interpersonal communication is covered by this chapter

- Biometric information collected, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, insurance, payment, or operations under HIPAA

- Scans and filming[11] of human anatomy used exclusively to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening

- Personal Information that meets the definition of:

    - Protected Health Information under HIPAA; or

    - Health care information captured from a patient by a provider or facility.

- Covered entities' publication of entity-based member or employee contact information where such publication is intended to allow member of the public to contact such member or employee in the ordinary course of the entity's operations

❖ A covered entity shall not be required to provide meaningful notice or obtain consent when:

- Processing is necessary to execute the specific transaction for which the individual is providing personal information.

- The covered entity believes that (i) an emergency involving immediate danger of death or serious physical injury to any individual requires obtaining without delay personal information so that it can be used to respond to the emergency; and (ii) the request is narrowly tailored to address the emergency, subject to the following limitations.

    - The request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to an individual requires obtaining without delay captured personal information relating to the emergency; and

[11] Includes X-ray roentgen process, computed tomography, MRIs, PET scans, mammographies, and "other image or film of human anatomy."

- Simultaneously with obtaining the captured personal information, the covered entity shall use reasonable efforts to inform the individual of the captured personal information obtained; the details of the emergency; and the reasons why the entity needed to obtain the personal information and shall continue such effort to inform until the receipt of information is confirmed.

➢ Processing involves only de-identified information, provided that a covered entity that processes de-identified information must:

- Have a privacy policy that details how de-identified information is processed;
- Implement technical safeguards that prohibit indirect re-identification of the information;
- Implement business processes that expressly prohibit indirect re-identification of the information;
- Implement business processes that prevent inadvertent release of de-identified information; and
- Not attempt to re-identify the information

❖ A covered entity in possession of biometric or location information need not destroy the information according to the proscribed retention schedule if issued a valid warrant by a court of competent jurisdiction.

❖ A covered entity, its affiliated data processors, or the third parties they contracted with shall not be required to obtain consent for disclosing or sharing personal information if:

➢ Disclosure is required to respond to a legal request, provided that:

- A covered entity receiving such legal request shall serve or deliver the following information to the individual to which the legal request for personal information refers by registered or first class mail, email, or other means reasonably calculated to be effective:

- A copy of the legal request and reasonably specific notice of the nature of the inquiry;
- That personal information related to the individual was supplied to, or requested by, a requesting entity and the date on which the supplying or requesting took place;
- An inventory of the supplied or requested personal information;
- Whether the information was in possession of the covered entity, an affiliated processor, or a third-party they contracted with; and
- The identity of the person that sought the legal request from the court, if known.

- Such notification must be delivered immediately upon receiving the legal request unless a delay is ordered in accordance with this chapter. Please see full text above for details.

❖ Because the covered entity may not request consent from a consumer that has refused to give it for six months, the covered entity may retain the consumer's personal information only as necessary to comply with this waiting period.

❖ A covered entity may process an individual's biometric or location information to recommend actions, goods, services, or products provided that:

➢ There is a full disclosure to the individual about the biometric or location information processed;

➢ Consent was given in a manner consistent with this section; and

➢ There is full disclosure that such recommendation is based on the biometric or location information processed.

❖ A covered entity can process or cause to process an individual's personal information acquired from a third party without the individual's consent if the processing is necessary to obtain consent, and provided the covered entity shall

➢ Process only the personal information required to request consent;

- Process the personal information solely to request consent; and
- Immediately delete the personal information if consent is not given.

Vendor Provisions

- Covered entities and data processors have duties of care, loyalty, and confidentiality to the individual whose personal information is processed
- A covered entity shall not disclose personal information to a data processor or another third party without a contractual agreement that:
  - Imposes the same duties of care, loyalty, and confidentiality on the third party as the covered entity has toward the individual;
  - Requires the data processor or third party to meet the same privacy and security obligations as the covered entity;
  - Prohibits the data processor or third party from processing the personal information for any purpose other than the purposes for which the individual provided consent; and
  - Prohibits the data processor or third party from further disclosing or processing the personal information except as explicitly authorized by the contract and consistent with this chapter.
- Covered entities shall regularly audit the data security and information practices of third parties and make the audit publicly available.
- If a covered entity learns that a data processor or third party to whom it has provided access to personal information is using such information in violation of this chapter, the covered entity shall immediately:
  - Limit the violator's access to personal information;
  - Seek proof of destruction of personal information previously accessed by the violating data processor or third party; and

- Notify the Commission about the violation

Massachusetts

An Act Relative to Consumer Data Privacy

- Legislative Status: Study Order Issued
- Link to Text: S 120

Massachusetts Consumer Rights Checklist	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who resides in Massachusetts.

- ***Personal Information*** means any information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device.

  Personal Information does not include consumer information that is identified or aggregate consumer information.

- ***Business*** means a for-profit legal entity that collects Massachusetts consumers' personal information; and satisfies one or more of the following thresholds:

  - Has annual gross revenues in excess of $10 million; or

  - Derives 50% or more of its annual revenues from third party disclosure of consumers' personal information

- A ***Business*** also refers to any entity that controls or is controlled by a business, as defined above, and shares common branding with the business.

Enforcement

- The Attorney General may bring an action for a temporary restraining order or an injunction. In addition, the Attorney General may seek a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

- ***Private Right of Action***

  - A consumer may bring a civil action for any of the following:

    - Damages in the amount not greater than $750 per incident or actual damages
    - Injunctive or declaratory relief
    - Reasonable attorney fees and costs
    - Any other relief the court deems proper

Data Safe Harbors

- A business collecting or disclosing personal information of the business's employees so long as information is within scope of its role as employer

- Health information collected by a covered entity or business associate governed by the privacy, security and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164

- A covered entity governed by the privacy, security and breach notification rules under the HIPAA

- Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects

- Sale of personal information to or from a consumer reporting agency if information is to be used to generate a consumer report under the Fair Credit Reporting Act

- Personal information collected, processed, sold or disclosed under the GLBA
- Personal information collected, processed, sold or disclosed under the Driver's Privacy Protection Act
- Education information covered by the Federal Family Educational Rights and Privacy Act

There are no ***Vendor Provisions***

Minnesota

Minnesota Consumer Data Privacy Act

- Date Introduced: 2/16/2021
- Link to Text: HF 1492
- Effective Date: July 31, 2022[12]
- Status: Referred to the Committee on Commerce Finance and Policy

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction[13]		✓

Key Definitions

- ***Consumer*** means a natural person who is a Minnesota resident acting only in an individual or household context.

- ***Controller*** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controller also means legal entities that conduct business in Minnesota or produce products or services that are targeted to residents of Minnesota, and that satisfy one or more of the following thresholds:

    - During a calendar year, controls or processes personal data of 100,000 consumers or more

[12] Except that certain nonprofits, air carriers, and postsecondary institutions will not be required to comply until July 31, 2026.
[13] "Delete means to remove or destroy information such that it is not maintained in human or machine readable form and cannot be retrieved or utilized in the course of business."

- Derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more

- ***Personal Data*** means any information that is linked or reasonably linkable to an identified or identifiable person.

- ***Personal Data*** does not include de-identified data or publicly available information.

- ***Consent*** means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose.

Enforcement

- The Attorney General may bring action seeking injunctive relief, up to $7,500 civil penalties for each violation and the state's litigation expenses incurred.

- The Attorney General must provide the controller or processor with a warning letter specifying the alleged violations and may only bring an action if the Attorney General believes there has been a failure to cure after 30 days.

- There is no ***Private Right of Action***

Data Safe Harbors

- This act does not apply to government entities.

- This act does not apply to federally recognized Indian tribes.

- Information that meets the definition of:

  - Protected Health Information under HIPAA

  - Health records as defined by section 144.291, subdivision 2

  - Patient identifying information for purposes of 42 C.F.R. Part 2;

- Identifiable private information for purposes of the Federal Policy for Protection of Human Subjects;
- Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986;
- Patient safety work product for purposes of 42 C.F.R. Part 3

❖ Information that is derived from any health care information listed above that has been de-identified in accordance with 45 C.F.R. Part 164

❖ Information originating from, and intermingled to be indistinguishable with any of the health care-related information listed above that is maintained by:

- A covered entity or business associate as defined by HIPAA
- A health care provider as defined by section 144.291, subdivision 2; or
- A program or a qualified service organization as defined by 42 C.F.R. Part 2

❖ Information used only for public health activities and purposes as described in 45 C.F.R. §164.512

❖ An activity involving the collection, maintenance, disclosure, sale, communication or use of any personal data bearing on a consumer's credit worthiness, credit capacity, character, general reputation, personal characteristics or mode of living pursuant to the Fair Credit Reporting Act

❖ Data collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act of 1994 or the Gramm-Leach-Bliley Act

❖ Personal data regulated by the Family Educational Rights and Privacy Act

❖ Personal data collected, processed, sold or disclosed pursuant to the Farm Credit Act of 1971

❖ Information maintained for emergency contact, job applicant, employment records, or benefit administration purposes

- Personal data collected, processed, sold or disclosed pursuant to the Minnesota Insurance Fair Information Reporting Act
- To comply with federal, state or local laws
- Comply with civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state or governmental authorities
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or local laws, rules or regulations
- Investigate, establish, exercise, prepare for or defend legal claims
- See full list at link provided above.

Vendor Provisions

- A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this chapter is not in violation of this chapter if the recipient processes such personal data in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.
- A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the obligations of the controller or processor from which it receives such personal data.
- A processor shall assist the controller to meet the controller's obligations under this chapter
- Processing shall be governed by the contract between the controller and processor and the contract must:
    - Set out the:

- Nature and purpose of the processing;
- The type of personal data subject to the processing;
- The duration of the processing; and
- The obligations and rights of both parties;

- Ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data;
- Allow the processor to engage a subcontractor only (i) after providing the controller with an opportunity to object; and (ii) pursuant to a written contract in accordance with the same statutory requirements that govern the contract between the controller and the processor that requires the subcontractor to meet the obligations of the processor with respect to the personal data;
- Provide that:
  - At the choice of the controller, the processor shall delete or return all personal data to the controller, unless the retention of personal data is required by law;
  - The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations of this chapter;
  - The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, and audit of the processor's policies and technical and organizational measure in support of this chapter's obligations. The auditor must use an appropriate and accepted control standard or framework and audit procedure for such audits as applicable, and shall provide a report of such audit to controller upon request.

Minnesota

Consumers given various rights regarding personal data, data transparency obligations placed on businesses, private right of action created, and enforcement provided by Attorney General

- Date Introduced: 1/7/2021
- Link to Text: HF 36
- Effective Date: June 30, 2022
- Status: Referred to Commerce Finance Policy

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared[14]		✓
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability[15]		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children[16]	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person.

- ***Personal Information*** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked directly or indirectly, with a particular consumer. This also includes inferences used to create a profile about the consumer drawn from personal information.

- ***Business*** means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, or any other legal or commercial entity that is organized or operated for the profit of financial benefit of the business's shareholders or other owners. To be subject to this chapter, the business (1) must meet

[14] Provides access to categories of information shared.
[15] Only if the business chooses to deliver the information electronically and data portability is technically feasible.
[16] Parent or child must affirmatively opt-in.

any of the following conditions itself or (2) control or be controlled by a separate business with which it shares common branding that meets any of the following conditions:

- Have gross revenues in excess of $25 million;
- Annually buy or sell the personal information of 50,000 or more consumers, households, or devices; or
- Derive 50% or more of the business's annual revenues from selling consumers' personal information.

- ***Business Purpose*** means the use of personal information for a business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information must be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected.
- ***Service Provider*** means a business to which another business discloses a consumer's personal information.
- ***Third Party*** means a business to which another business sells a consumer's personal information.

Enforcement

- The Attorney General may bring action seeking all the remedies and damages provided under the private right of action.
- ***Private Right of Action***
  - Any person injured by a violation of this chapter may bring a civil action to receive:
    - Damages not less than $100 and not greater than $750 per consumer, per violation, or the consumer's actual damages (whichever is greater);
    - The cost of investigation and reasonable attorney fees;
    - Other equitable relief as determined by the court; and

- Exemplary damages up to three times the other damages for willful and malicious violations.

Data Safe Harbors

- A business that discloses a consumer's personal information to a service provider or third party without violating this chapter shall not be liable for any subsequent violation by the service provider or third party unless the business had actual knowledge or reason to believe the service provider or third party intended to commit the violation.

- It is not a sale of personal information if:

  - A consumer directs the business to disclose the personal information to a third party (provided the third party does not sell the personal information);

  - A business uses or shares a consumer's identifier to inform a third party or service provider that the consumer has opted out; or

  - A business discloses a consumer's personal information to a service provider that is necessary to perform a business purpose and:

    - The business has provided notice that the information may not be disclosed;

    - The service provider does not further collect, sell, disclose, or use the personal information except as necessary to perform the business purpose; and

    - The business's contract with the service provider prohibits the service provider's retaining, using, or disclosing the personal information for any purpose other than the contracted purpose or a purpose permitted by this chapter.

  - A business transfers a consumer's personal information as an asset in the context of a merger, acquisition bankruptcy or other transaction where the third party assumes control of all or part of the business. However, use that is materially inconsistent with the terms agreed upon by the consumer requires that the consumer be given prior notice of the new or changed practice.

- In regard to access requests:

- A business may require authentication of a consumer's identity and request.
- A business is not required to:
  - Retain personal information collected for a single, one-time transaction (if such information is not sold or retained by the business); or
  - Re-identify or otherwise link information that is not maintained in a manner that would be considered personal information.[17]

- In regard to deletion; a business or service provider is not required to comply with a consumer's request if it is necessary for the business or service provider to maintain a consumer's personal information to:
  - Complete the transaction, fulfill the terms of a written warranty or product recall under federal law, provide a good or service requested by the consumer or reasonably anticipated within the context of a business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
  - Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;
  - Debug to identify or repair errors that impair existing intended functionality;
  - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
  - Enable solely internal uses that are reasonably aligned with the consumer's expectations based on the consumer's relationship with the business;
  - Comply with legal obligations; or

[17] This seems to be speaking of deidentified information, but the term is nowhere used.

- Use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information

- This act does not apply to nonprofit organizations or governmental entities.

Vendor Provisions

- A third party must not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to section 320.05.

- A service provider must not further retain, sell, disclose, or use the personal information except as necessary to perform the business purpose specified in the service provider's contract with the business or as otherwise permitted by law.

- A business that discloses a consumer's personal information to a service provider or third party without violating this chapter shall not be liable for any subsequent violation by the service provider or third party, provided that, at the time of disclosing the personal information, the business did not have actual knowledge or reason to believe, that the service provider or third party intended to commit the violation.

Mississippi

The Mississippi Consumer Privacy Act of 2021

- Legislative Status: Died in Committee
- Link to Text: SB 2612
- Effective Date: July 1, 2022

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared[18]		✓
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children[19]	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is not defined.

- ***Personal Information*** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household. Personal information includes, but is not limited to:

  - Identifiers such as real name, postal address, unique identifier, online identifier internet protocol address, email address, account name, SSN, driver's license number, passport number, etc.

  - Characteristics of protected classifications under Mississippi or federal law

[18] Categories only.
[19] If under 16, the consumer must opt-in. If 13-16, the parent or guardian must opt in.

- Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies
- Biometric information
- Internet or other electronic network activity information
- Geolocation data
- Audio, electronic, visual, thermal, olfactory or similar information
- Professional or employment-related information
- Education information, defined as information that is not publicly available personally identifiable information under the Family Educational Rights and Privacy Act
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer

❖ ***Personal Information*** does <u>not</u> include publicly available information.

❖ ***Business*** means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collect that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in Mississippi, and that satisfies one or more of the following thresholds:

- Has annual gross revenues in excess of $10 million
- Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, personal information of 50,000 or more consumers, households, or devices

- Derives 50% or more of its annual revenues from selling consumers' personal information.

❖ A ***Business*** is also defined as any entity that controls or is controlled by a business, as defined above, and shares common branding with the business.

Enforcement

❖ The Attorney General is authorized to enforce the act seeking civil penalties of up to $7,500 per violation if the business fails to cure within 30 days of notice.

❖ ***Private Right of Action***

- A consumer may bring an action seeking (1) actual damages or statutory damages of $100-$750 per incident (whichever is greater); (2) injunctive relief; or (3) any relief the court deems proper.

- Consumers must give businesses notice and 30 days to cure.

Data Safe Harbors

❖ This act does not apply to:

- Information subject to Fair Credit Reporting Act, HIPAA, GLBA, Driver's Privacy Protection Act

- De-identified or aggregate consumer information

❖ Nothing in the Act shall restrict a business's ability to:

- Comply with federal, state, or local laws;

- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;

- Cooperate with law enforcement concerning conduct or activity the business, service provider, or third party reasonably and in good faith believes may violate federal state or local law;

- Exercise or defend legal claims;
- Collect, use, retain, or disclose de-identified or aggregate consumer information; and
- Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of Mississippi.

❖ A business need not delete if the personal information is necessary to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible;
- Debug to identify and repair errors that impair existing intended functionality;
- Exercise free speech;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent; or
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

Vendor Provisions

❖ A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out.

New Hampshire

An Act Relative to the Collection of Personal Information by Businesses

- Legislative Status: Referred for Interim Study
- Link to Text: HB 1680
- Effective Date: 01/01/2021

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Business*** means:
  - A for-profit legal entity that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of New Hampshire, and that satisfies one or more of the following thresholds:
    - Has annual gross revenues in excess of $25 million
    - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices

- Derives 50% or more of its annual revenues from selling consumers' personal information

➢ Any entity that controls or is controlled by a business, as defined above, and that shares common branding with the business

❖ ***Consumer*** means a natural person who is a New Hampshire resident, however identified, including by any unique identifier.

❖ ***Personal Information*** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with or could be reasonably linked, directly or indirectly, with a particular consumer or household:

➢ Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number or other similar identifiers

➢ Information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number or any other financial information, medical information or health insurance information

➢ Characteristics of protected classifications under New Hampshire or federal law

➢ Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies

➢ Biometric information

➢ Internet or other electronic network activity information, including, but not limited to browsing history, search history and information regarding a consumer's interaction with an internet web site, application or advertisement

- Geolocation data
- Audio, electronic, visual, thermal, olfactory or similar information
- Professional or employment-related information
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act
- Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes

❖ ***Personal Information*** does not include publicly available information.

Data Safe Harbors

❖ Comply with federal, state or local laws

❖ Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state or local authorities

❖ Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law

❖ Exercise or defend legal claims

❖ Collect, use, retain, sell or disclose consumer information that is de-identified or in the aggregate consumer information

❖ Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of New Hampshire

- Medical information governed by RSA 332-I or Protected Health Information that is collected by a covered entity or business associate governed by the privacy, security and breach notification rules established under HIPAA

- A provider of health care or a covered entity governed by the privacy, security and breach notification rules established under HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or Protected Health Information as described above

- Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects

- Information subject to Fair Credit Reporting Act, HIPAA, GLBA, Driver's Privacy Protection Act

Enforcement

- ***Attorney General***

  - The Attorney General may seek an injunction and a civil penalty of no more than $2,500 for each violation or $7,500 for each intentional violation.

- ***Private Right of Action***

  - Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

    - To recover damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater;

    - Injunctive or declaratory relief;

    - Any other relief the court deems proper.

Vendor Provisions

- A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out.

New Jersey

Senate Bill 269[20]

- Legislative Status: Introduced 1/14/2020, referred to Senate Commerce Committee
- Link to Text: S 269

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Data subject*** means an individual within New Jersey who provides, either knowingly or unknowingly, personally identifiable information to a business.

- ***Personal Identifiable Information*** means any information that personally identifies, describes, or is able to be associated with a data subject, including but not limited to:

  - Name, alias, nickname and user name
  - Postal and electronic mail address
  - Telephone number
  - Account name

[20] Last session bill number: S 3153, identical to Assembly bill 4640

- Social Security number or other government-issued identification number, birthdate or age
- Physical characteristic information, including height and weight
- Biometric data
- Sexual information (including sexual orientation, sex, gender status)
- Race or ethnicity
- Religious affiliation or activity
- Political affiliation or activity
- Professional or employment-related information
- Educational information
- Medical information
- Financial information
- Commercial information (including records of property, products or services provided, obtained or considered, or other purchasing or consumer histories)
- Geolocation information
- Internet or mobile activity information, including IP addresses or information concerning the access or use of any online service
- Content, including text, photographs, audio or video recordings, or other material generated by or provided by the data subject

- Any of the above categories of information concerning children of the data subject.

- ***Business*** means a corporation, partnership, firm, enterprise, franchise, association, trust, sole proprietorship, union, political organization or other legal entity other than a state agency (or any subdivision or contractor thereof) or federal agency that does business in New Jersey and has:

  - Annual gross revenue of $5 million or more

  - Derives 50% or more of its annual revenue from selling the personally identifiable information of data subjects; or

  - Alone or in combination, annually buys, receives, sells or shares for commercial purposes the personally identifiable information of at least 25,000 data subjects

Enforcement

- ***Private Right of Action***

  - A consumer may bring a civil action of not less than $100 and not more than $750 per security incident.

Data Safe Harbors

- The requirements imposed shall not restrict a business's ability to:

  - Comply with federal, state or local law

  - Comply with a civil, criminal or regulatory inquiry, investigation or summons by federal, state or local authorities

  - Cooperate with law enforcement agencies or exercise or defend legal claims; or

  - Collect, use, retain, sell or disclose a data subject's personally identifiable information that has been de-identified or in aggregate data subject information

Vendor Provisions

- Although a business must allow a data subject to opt out of processing its personally identifiable information (PII), this requirement does not apply where the processing of a data subject's PII occurs pursuant to a written contract between a business and third party, and where that contract prohibits the third party from using the PII for any reason other than performing the specified service and from disclosing PII to additional third parties.

New Jersey

Assembly Bill 3255

- Legislative Status: Introduced 2/25/2020, Referred to Assembly Science, Innovation and Technology Committee
- Link to Text: A3255

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Data subject*** means an individual within New Jersey who provides, either knowingly or unknowingly, personally identifiable information to a business.

- ***Personal Identifiable Information*** means any information that personally identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, to a consumer or household, including, but not limited to:

  - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, electronic mail address, account name, Social Security number, driver's license number, passport number or other similar identifiers

  - Characteristics of protected classifications under state or federal law

- Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies
- biometric information
- Internet or other electronic network activity information, including, but not limited to browsing history, search history and information regarding a consumer's interaction with an internet website, application or advertisement
- Geolocation data
- Audio, electronic, visual, thermal, olfactory or similar information
- Professional or employment-related information
- Education records, defined as information that is not publicly available personally identifiable information, as defined in the Family Educational Rights and Privacy Act of 1974, (20 U.S.C. s.1232g)
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes

❖ ***Business*** means a for-profit legal entity that collects consumers' personally identifiable information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personally identifiable information, that does business in this state, and that satisfies one or more of the following thresholds:

- An annual gross revenue of $25 million or more
- Derives 50% or more of its annual revenue from selling the personally identifiable information of data subjects

- Alone or in combination, annually buys, receives, sells or shares for commercial purposes the personally identifiable information of at least 50,000 consumers

Enforcement

- A business is to be liable to an affected data subject for any violation for a civil penalty of not less than $100 and not more than $750 per data subject per security incident, or actual damages, whichever is greater, and may be recoverable by the data subject in a civil action in a court of competent jurisdiction, which may also order injunctive relief or any other relief the court deems necessary.

Data Safe Harbors

- The requirements imposed shall not restrict a business's ability to:
  - Comply with federal, state or local law
  - Comply with a civil, criminal or regulatory inquiry, investigation or summons by federal, state or local authorities
  - Cooperate with law enforcement agencies or exercise or defend legal claims
  - Collect, use, retain, sell or disclose a data subject's personally identifiable information that has been de-identified or in aggregate data subject information
  - Collect or sell a consumer's personally identifiable information if every aspect of that commercial conduct takes place wholly outside of the state

There are no ***Vendor Provisions***

New Jersey

Assembly Bill No. 3283

- Legislative Status: Introduced 02/25/2020
- Link to Text: A3283

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out		✓
Children		✓
Data Destruction		✓
Opt In	✓	

Key Definitions

- ***Business*** is not defined.
- ***Consumer*** means an individual in this state who provides, either knowingly or unknowingly, personally identifiable information to a controller.
- ***Controller*** means a person or legal entity that collects, maintains, and determines the purposes and means of processing personally identifiable information.
- ***Personally identifiable information*** means any information that is linked or reasonably linkable to an identified or identifiable consumer, including a minor child in the custody of the consumer. "Personally identifiable information" shall not include de-identified information or publicly available information.

Enforcement

- ***Attorney General***

- The Attorney General may take legal action and will appoint a head of the Office of Data Protection and Responsible Use in the Division of Consumer Affairs in the Department of Law and Public Safety.

❖ ***No Private Right of Action***

Data Safe Harbors

❖ A consumer is to have the right to object, by any means, to the processing of personally identifiable information, at which time the controller is to no longer to process the personally identifiable information unless the controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights, and freedoms of the consumer or for the establishment, exercise, or defense of legal claims.

❖ The bill provides that where personally identifiable information is processed for scientific or historical research purposes or statistical purposes, the consumer is to have the right to object, by any means, to the processing of their personally identifiable information unless the processing is necessary for the public interest.

Vendor Provisions

❖ A controller that discloses a consumer's personally identifiable information to a processor or third party shall make the following information available to the consumer free of charge upon receipt of a verified request from the consumer for this information through a designated request address:

- The purposes of the processing;
- The category or categories of a consumer's personally identifiable information that were disclosed;
- The category or categories of the processors and third parties that received the consumer's personally identifiable information;
- Where possible, the period of time for which the personally identifiable information will be stored by the controller, processor, or third party, or, if not possible, the criteria used to determine that period of time;

- If personally identifiable information was not obtained directly from a consumer, any available information concerning the source of that consumer's personally identifiable information;
- The existence of automated decision making, including profiling, and information about the logic involved, and the significance and consequences of this processing to the consumer; and
- A copy of the personally identifiable information undergoing processing. For more than a single copy, the controller may charge a reasonable fee based on administrative costs.

New Mexico

Consumer Information Privacy Act

- Legislative Status: action postponed indefinitely in Senate.
- Link to Text: SB 176

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is not specifically defined by the statute.
  - However, Section 7 of the act sets forth certain limitations in scope, which are relevant to how the definition of consumer is construed. The act does not apply to the collection or sale of personal information if "every aspect of the business's commercial conduct occurs wholly outside the state." Commercial conduct takes place wholly outside of the state if the business collected that information while the consumer was outside of the state, no part of the sale of the consumer's personal information occurred in the state and no personal information collected while the consumer was in the state is sold.

- ***Personal Information*** is defined as information from federal, state or local government records that identifies, describes or could reasonably be linked with a particular consumer or household, including:
  - A real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, bank account number, credit card number,

debit card number, driver's license or state identification card number, insurance policy number, Social Security number, passport number or telephone number

- Any information that identifies or is capable of being associated with a particular individual, including a signature, physical characteristic or description, education, employment, employment history, financial information, medical information or health insurance information
- Characteristics of protected classifications under state or federal law
- Commercial information, including records of personal property, purchases of products or services or histories of purchases
- Biometric information
- Internet or other electronic network activity information
- Geolocation data
- Audio, electronic, visual, thermal, olfactory or similar information
- Inferences drawn from any of the information identified above to create a profile about a consumer that reflects the consumer's preferences, characteristics, psychological trends, behaviors, predispositions, attitudes, intelligence, abilities or aptitudes

Personal Information does <u>not</u> include publicly available information.

- ***Business*** means a corporation, joint venture, limited liability company, partnership, limited partnership, limited liability partnership, real estate investment trust or sole proprietor; or an entity that is controlled by any such entity.

Enforcement

- ***Attorney General***
  - The Office of the Attorney General may bring civil enforcement actions for violations.

- ***Private Right of Action***

  - Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may file a civil action to recover actual damages; for injunctive relief; for statutory damages up to $750 per single occurrence or any other relief deemed proper by the court. Any action for statutory damages must comply with certain procedural requirements.

Data Safe Harbors

- To comply with federal, state or local laws
- To comply with civil, criminal or regulatory inquiry, an investigation, a subpoena or a summons by federal, state or local authorities
- To cooperate with law enforcement agencies concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law
- To exercise or defend legal claims
- To collect, use, retain, sell or disclose consumer information that is de-identified or is in aggregate consumer information
- To collect or sell a consumer's personal information if every aspect of the business' commercial conduct takes place wholly outside of the state

Vendor Provisions

- The New Mexico bill prohibits a third party from selling personal information about a consumer that was sold to the third party by a business, unless the consumer received explicit notice and is provided an opportunity to exercise the right to opt out of the sale.

- Upon receipt of a request to delete the consumer's personal information from its records, the business must notify any service providers to delete the consumer's personal information from their records.

New York

Right to Know Act

- Legislative Status: In Committee
- Link to Text: SB 224

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required		✓
Opt Out		✓
Children		✓
Data Destruction		✓

Key Definitions

- ***Customer*** is defined as a New York resident who provides personal information to a business. An individual is also a customer of a business if that business obtained the individual's personal information from any other business.

- ***Personal Information*** is defined as any information that identifies or references a particular individual or electronic device or any information that relates to or describes an individual if disclosed in connection with identifying/referencing information. The definition includes name, alias, address, phone number, email, IP address, account name, SSN, driver's license number, passport number and any other identifier intended to be uniquely associated with a particular individual or device.

- ***Business*** is defined as any person, proprietorship, firm, partnership, cooperative, nonprofit organization or corporation organized or existing under the laws of any state and "doing business" in New York.

Enforcement

- Civil actions to recover penalties may be brought by the Attorney General, a district attorney, a city attorney, or a city prosecutor.

- ***Private Right of Action***

  - Civil actions to recover penalties may be brought by a customer.

There are no ***Data Safe Harbors***

There are no ***Vendor Provisions***

New York

New York Privacy Act

- Legislative Status: In Committee
- Link to Text: SB 5642
- Same as: AB 8526
- 2021-2022 Version: A680

Consumer Rights	Yes	No
Access to Personal Information Collected	❖	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is a New York resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

- ***Personal Data*** means information relating to an identified or identifiable natural person. Personal data includes:

  - An identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, internet protocol address, email address, account name, mother's maiden name, Social Security number, driver's license number, passport number or other similar identifier

  - Information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other

financial information, medical information, mental health information or health insurance information

- Commercial information, including a record of personal property, income, assets, leases, rentals, products or services purchased, obtained, or considered or other purchasing or consuming history
- Biometric information, including a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry
- Internet or other electronic network activity information, including browsing history, search history, content, including text, photographs, audio or video recordings, or other user generated-content, non-public communications, and information regarding an individual's interaction with an internet website, mobile application, or advertisement
- Historical or real-time geolocation data
- Audio, electronic, visual, thermal, olfactory, or similar information
- Education records
- Political information or information on criminal convictions or arrests
- Any required security code, access code, password, or username necessary to permit access to the account of an individual
- Characteristics of protected classes under the human rights law, including race, color, national origin, religion, sex, age, or disability
- An inference drawn from any of the information described in this paragraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities or aptitudes

- ***Business*** means any person, proprietorship, firm, partnership, cooperative, nonprofit organization or corporation organized or existing under the laws of any state and "doing business" in New York.

Enforcement

- The Attorney General may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this article.

- ***Private Right of Action***

  - Any person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions. The court may award reasonable attorney's fees to a prevailing plaintiff.

Data Safe Harbors

- The obligations imposed on controllers or processors under this article do not restrict a controller's or processor's ability to:

  - Comply with federal, state or local laws

  - Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, local or other governmental authorities

  - Disclose personal data to a law enforcement agency

  - Cooperate with a governmental entity

  - Investigate, exercise or defend legal claims

  - Prevent or detect identity theft, fraud or other criminal activity or verify identities

Vendor Provisions

- Processing by a processor shall be governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

New York

- Legislative Status: Introduced and Referred to Consumer Protection January 6, 2021
- Link to Text: SB 567

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Business*** means either
  - A for-profit legal entity that collects consumer's personal information, does business in New York, and satisfies one or more of the following:
    - Has annual gross revenues in excess of $50 million;
    - Annually sells, alone or in combination, the personal information of 100,000 or more consumers or devices; or
    - Derives 50% or more of its annual revenues from selling consumers' personal information; or
  - Any entity that controls or is controlled by a business and that shares common branding with the business.
- ***Consumer*** means a natural person who is a resident of New York.

- ***Personal Information*** means information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device, including, but not limited to:

  - Any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, alias, signature, Social Security number, physical characteristics or description, address, electronic mail address, internet protocol address, unique identifier, account name, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information;

  - Characteristics of protected classifications under state or federal law;

  - Commercial information, including records of property, products or services provided, obtained, or considered, or other purchasing or consuming histories or tendencies;

  - Biometric data;

  - Internet or other electronic network activity information, including but not limited to, browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;

  - Geolocation data;

  - Audio, electronic, visual, thermal, olfactory, or similar information;

  - Psychometric information;

  - Professional or employment-related information;

  - Inferences drawn from any of the information identified above; and

  - Any of the categories of information set forth in this subdivision as they pertain to the minor children of the consumer.

Personal Information does not include information that is publicly available or that is de-identified.

Enforcement

- ***Attorney General***
  - The Attorney General may enforce civil actions for violations.
- ***Private Right of Action***
  - Any consumer who suffers an injury in fact shall recover statutory damages in the amount of $1,000 or actual damages, whichever is greater, for each violation from the business or person responsible for the violation, except that in the case of a knowing and willful violation by a business or person, an individual shall recover statutory damages of not less than $1,000 and not more than $3,000, or actual damages, whichever is greater, for each violation from the business or person responsible for the violation.

Data Safe Harbors

- Compliance with federal, state, or local laws;
- Compliance with a civil, criminal, or regulatory investigation or subpoena or summons by federal, state, or local authorities;
- Cooperation with law enforcement agencies concerning conduct or activity that the business reasonably and in good faith believes may violate federal, state, or local law;
- In-state collection and sale of a consumer's personal information
- Where compliance would violate an evidentiary privilege under state law
- Personal information collected by a covered entity under HIPAA
- Personal information to or from a consumer reporting agency under the Fair Credit Reporting Act.

Vendor Provisions

- Third parties to whom a business discloses consumer's personal information must be for a business purpose pursuant to a written contract that prohibits the person receiving the personal information from:
  - Selling the personal information;
  - Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract;
  - Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business;
  - Includes a certification by the person receiving the personal information that they understand these restrictions.

New York

Digital Fairness Act

- Legislative Status: In Committee, March 5, 2021
- Link to Text: A6042

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out		✓
Children		✓
Data Destruction	✓	
Opt In	✓	

Key Definitions

- ***Covered Entity*** means a legal entity that conducts business in New York state and as part of such business, processes and maintains the personal information of 500 or more unique individuals.

- ***Individual*** means a natural person whom a covered entity knows or has reason to know is located within New York state.

- ***Personal Information*** means information that is captured in exchange for any kind of value provided to the individual to whom the information pertains, including but not limited to a good or service, the placement of targeted advertisements, or a membership; as a result of an individual, household, or device's establishment or maintenance of an account with a covered entity; or as a result of an individual, household, or device's interaction with a covered entity. Personal Information also includes information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device that provides or provided information to a covered entity in exchange for any kind of value provided to

the individual to whom such information pertains or that established, maintained, establishes or maintains an account with a covered entity. Information is reasonably linkable to an individual, household, or device if it can be used on its own or in combination with other reasonably available information, regardless of whether such other information is held by the covered entity, to identify an individual, household, or device.

- ***Third Party*** shall mean, with respect to an individual's personal information, any person that is not the covered entity or a data processor.

Enforcement

- ***Attorney General***
  - The Attorney General may bring an action in the name of the state, or as a *parens patriae* proceeding on behalf of persons residing in the state, to enforce this article. In such action, the court may award injunctive relief, civil penalties, or any other relief the court deems appropriate.
- ***Private Right of Action***
  - Any individual may bring a civil action in any court of competent jurisdiction alleging a violation of this article, or a violation of a rule or regulation promulgated to effectuate the provisions of this article.

There are no ***Data Safe Harbors***

- A covered entity shall not be required to obtain freely given, specific, informed, and unambiguous opt-in consent from an individual under subdivision one of this section if:
  - The processing is necessary for the primary purpose of the transaction for which personal information is provided;
  - The covered entity, in good faith, believes that an emergency presenting the risk of death or serious physical injury to any individual requires disclosure, without delay, of personal information relating to such emergency, the covered entity may disclose the personal information relating to such emergency to a governmental entity;

- Processing the personal information is necessary for engaging in public or peer-reviewed scientific, medical, historical, social science, or statistical research in the public interest that adheres to all other applicable ethical standards or laws, with informed consent;

- Processing the personal information is necessary for clinical, treatment, public health, medical educational, medical training, or insurance purposes, provided that the personal information shall not be processed or monetized for any other purpose without the freely given, specific, informed, and unambiguous opt-in consent from such individual to whom the personal information pertains;

- The processing involves only de-identified information;

- In response to a warrant issued by a court of competent jurisdiction under the procedures described in the federal rules of criminal procedure or Article 690 of the criminal procedure law;

- If required by state or federal law.

Vendor Provisions

- A covered entity shall not disclose personal information to a third party unless that third party is contractually bound to the covered entity to meet the same privacy and security obligations as the covered entity.

- A covered entity shall not disclose personal information to a data processor unless the covered entity enters into a contractual agreement with such data processor that prohibits the data processor from processing such personal information for any purpose other than the purposes for which the individual provided the personal information to the covered entity, and that requires the data processor to meet the same privacy and security obligations as the covered entity. Such data processor shall not further disclose or process personal information it has acquired from the covered entity except as explicitly authorized by the contract.

North Dakota

A bill for an Act to create and enact chapter 51-37 of the North Dakota Century Code, relating to protection against the disclosure of personal information; and to provide a penalty.

- Legislative Status: Passed
- Link to Text: HB 1485

Consumer Rights	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required		✓
Opt In		✓
Opt Out		✓
Children		✓
Data Destruction		✓

Key Definitions

- ***Covered Entity*** means a partnership, limited liability company, corporation, or other legal entity, including a social media company, that sells a user's protected data and does business in the state and:
  - Has annual gross revenues in excess of $25 million;
  - Annually buys, receives, sells, or shares personal information of at least 50,000 consumers, households, or devices, or
  - Derives at least 50% of its annual revenues from selling personal information.

- ***Personal Information*** means information that identifies, describes, or could reasonably be linked with a particular individual, including:

  - Personal identifiers including real name, alias, postal address, unique personal identifier, online identifier internet protocol address, electronic mail address, account name, Social Security number, date of birth, operator's license number, passport number, or other similar identifier.

- Biometric information
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. Internet or other electronic network activity information, including browsing history, search history, and information regarding an individual's interaction with an internet website, application, or advertisement.
- Geolocation data.
- Inferences drawn from any of the information identified in this subsection to create a profile about a consumer reflecting the individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Personal Information does not include publicly available information lawfully made available to the general public from federal, state, or local government records.

Enforcement

- ***Attorney General***
  - The Attorney General has authority to enforce and impose civil penalties.
- ***Private Right of Action***
  - If an individual's personal information is purchased, received, sold, or shared by a covered entity in violation of this chapter, the individual may bring a civil action in a court of this state with jurisdiction over the covered entity to recover damages, costs, and fees, including reasonable attorneys' fees; or obtain injunctive or declaratory relief; or any other relief the court deems proper.

Data Safe Harbors

- Disclosure to any person pursuant to a subpoena or court order;

- Disclosure that is discoverable pursuant to the North Dakota Rules of Civil Procedure;
- Disclosure to any person pursuant to a lawful search warrant; or
- Disclosure required by law.

No Vendor Provisions

Oklahoma

Data transparency; defining terms; requiring online business or website to make posting of certain consumer information to be collected

- Legislative Status: Second Reading referred to House Rules Committee
- Link to Text: HB 1130
- Effective: November 1, 2021

Consumer Rights	Yes	No
Access to Personal Information Collected		✓
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion		✓
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out		✓
Opt In		✓
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** means an individual who is a resident of Oklahoma.

- ***Personal Information*** means information that identifies, relates to, describes, is capable of being associated with or can reasonably be linked to, directly or indirectly, a particular consumer or household:

  - Identifiers (e.g., name, address, usernames, email addresses, account names, Social Security numbers, driver's license numbers, etc.)

  - Characteristics of protected classifications

  - Commercial information (e.g. records of personal property, products or services purchased, etc.)

- Biometric information
- Internet or network activity
- Geolocation data
- Audio/electronic/visual/thermal/olfactory information
- Professional or employment-related information
- Education or financial information;
- Inferences drawn from any of the above to create a "profile about a consumer" that reflect preferences, psychological trends, behaviors, etc.

❖ ***Business*** means a sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information, or on the behalf of which such information is collected, and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of Oklahoma.

Enforcement

❖ The Attorney General may promulgate rules to effectuate the provisions of this section.

❖ Failure to cure any alleged violation within 30 days subjects the business, service provider, or other person to fines of $1,000 for the first violation and $5,000 for each additional violation.

❖ This act nowhere mentions a ***Private Right of Action.***

Data Safe Harbors

❖ This act does not apply to (1) nonprofits; (2) governmental entities; or (3) publicly available information

Vendor Provisions

- This act does not create specific vendor provisions.

Oklahoma

Oklahoma Computer Data Privacy Act

- Legislative Status: Second Reading Referred to Judiciary Committee
- Link to Text: HB 1602

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared[21]	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability[22]	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Opt In[23]	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Consumer*** means an individual who is a resident of Oklahoma.

- ***Personal Information*** means information that identifies, relates to, describes, can be associated with or can reasonably be linked to, directly or indirectly, a particular consumer or household:

  - Identifiers (e.g., name, address, usernames, email addresses, account names, Social Security numbers, driver's license numbers, etc.)

  - Online identifiers (e.g. email, IP address, etc.)

  - Physical characteristics

[21] The right provides access the categories of information shared, but then clarifies that the information must be provided. § 20(C)(1).
[22] *See* § 20(C)(2)(a); (D).
[23] A consumer must opt in before a business can sell that consumer's information.

- Characteristics of protected classifications
- Commercial information (e.g. records of personal property, products or services purchased, etc.)
- Biometric information
- Internet activity
- Geolocation data
- Audio/electronic/visual/thermal/olfactory information
- Professional or employment-related information
- Education or financial information;
- Inferences drawn from any of the above to create a "profile about a consumer" that reflect preferences, psychological trends, behaviors, etc.

❖ ***Business*** means a for-profit legal entity, including a sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or financial benefit of the entity's shareholders or other owners.

❖ ***Business*** does not include internet service providers so long as they are acting in their role as internet service providers.

Enforcement

❖ The Attorney General may bring a civil action to recover civil penalties, injunctive relief, reasonable attorney fees, court costs, and investigatory costs.

❖ Civil penalties are in amounts not to exceed $2,500 per violation, or $7,500 for intentional violations.

- This act nowhere mentions a ***Private Right of Action.***

Data Safe Harbors

- This act applies to
  - Businesses that:
    - Do business in the state;
    - Collect consumers' personal information or have that information collected on the business's behalf;
    - Alone, or in conjunction with others, determine the purpose for and means of processing consumers' personal information; and
    - Satisfy one or more of the following thresholds:
      - Annual gross revenue greater than $10 million
      - Alone or in combination with others, buys, sells or receives for a commercial purpose the personal information of 50,000 consumers, households, or devices; or
      - Derives 25% or more of annual revenue from selling consumers' personal information.
  - Entities that controls or are controlled by a business meeting the requirements above and that share the same or substantially similar branding and/or a common customer database
- This act does not apply to:
  - Nonprofits or governmental entities
  - Publicly available information

- Information and business associates governed under state or federal health laws including HIPAA, the federal Health Information Technology for Economic and Clinical Health Act, and Title XIII of the federal American Recovery and Reinvestment Act of 2009, to the extent the use complies with these laws

- Providers, covered entities, and health plans governed by state privacy health laws or HIPAA to the extent the provider or covered entity complies with those laws

- Information meeting the de-identification requirements in 45 C.F.R. 164.514 and derived from patient information that was originally collected, created, transmitted or maintained by an entity regulated under HIPAA or the Federal Police for the Protection of Human Subjects, to the extent it is not re-identified

- Information used to create or reported in a consumer report and complying with the Fair Credit Reporting Act and solely used under that act

- Personal information collected, processed, sold, or disclosed under:

  - Gramm-Leach-Bliley Act (GLBA) of 1999 and its regulations; or

  - The federal Driver's Privacy Protection Act of 1994

- De-identified or aggregate consumer information

- A consumer's collected personal information if every aspect of the collection or sale occurred wholly out of the state

- Financial institutions or their affiliates under the GLBA

- Noncommercial activities of a person connected with or employed by a periodical, a radio or television station licensed under the FCC, or an entity that provides an information service, including a press association or wire service

❖ Information that meets the definition:

- Of research in 45 C.F.R. 164.501 and that complies with the Federal Policy for the Protection of Human Subjects, good clinical practice guidelines under the

International Council for Harmonisation, or human protection requirements under the FDA

- This act does not interfere with a business's ability to
  - Comply with
    - Applicable federal, state, or local laws; or
    - A civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, or local authority
  - Cooperate with a law enforcement agency concerning conduct that the business, a service provider, or a third party reasonably and in good faith believes may violate other applicable federal, state, or local laws
  - Pursue or defend against a legal claim
  - Detect a security incident, protect against malicious, deceptive, fraudulent or illegal activity; or prosecute those responsible for the illegal activity described above
  - Assist another party with any of the foregoing
  - Violate an evidentiary privilege under federal or state law
- This act does not require a business to:
  - Retain a consumer's personal information that was collected for a one-time transaction if the information is not sold or retained in the ordinary course of business
  - Re-identify or otherwise link any data, that in the ordinary course of business, is not maintained in a manner that would be considered personal information
  - Comply with unverified requests

- This act does not require a business or service provider to comply with a verified consumer request to delete information if the business or service provider needs to retain the consumer's personal information to:
    - Comply with a consumer's opt-out request;
    - Complete the transaction for which the information was collected;
    - Provide a good or service requested by the consumer in the context of the ongoing business relationship;
    - Perform under a contract between the business and the consumer;
    - Detect a security incident; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such illegal activity;
    - Identify and repair or remove errors from computer hardware or software that impair its intended function;
    - Exercise free speech or ensure the right of another consumer to exercise the right of free speech or another right afforded by law;
    - Comply with a court order or subpoena or other lawful process; or
    - Engage in peer-reviewed scientific, historical, or statistical research that is in the public interest and that adheres to all other applicable ethics and privacy laws, provided that:
        - The business's deletion is likely to render impossible or seriously impair the achievement of the research; and
        - The consumer has previously provided to the business informed consent to retain the information for such use.

Vendor Provisions

- A third party shall not sell personal information about a consumer that was sold to the third party by a business unless the consumer received explicit notice of the potential sale and is provided an opportunity to, and in fact does, opt in.

- A service provider may not be held liable for a violation of this act by the business.

- A business that discloses to a third party, or to a service provider for a business purpose, is not liable for a violation by the third party or service provider unless the business had actual knowledge or a reasonable belief that the third party or service provider intended to violate this act.

- A business must have a written contract with a service provider that:

    - Prohibits the service provider retaining, using or disclosing the information for any purpose other than:

        - Providing the services specified in the contract; or

        - For a purpose permitted by this act, including for a commercial purpose other than providing those specified services.

Pennsylvania

Consumer Data Privacy Act

- Legislative Status: Died in Committee
- Link to Text: HB 1049

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** is not specifically defined in the statute.

- ***Personal Information*** is defined as information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked to either a particular consumer or household and includes:

  - Identifiers (e.g., name, address, usernames, email addresses, account names, Social Security numbers, driver's license numbers, etc.)

  - Characteristics of protected classifications

  - Commercial information (e.g. records of personal property, products or services purchased, or other purchasing or consuming history)

  - Biometric information

  - Internet activity

- Geolocation data
- Audio/electronic/visual/thermal/olfactory information
- Professional or employment-related information
- Education information; and
- Inferences drawn from any of the above to create a "profile about a consumer" that reflect preferences, psychological trends, behaviors, etc.
- Personal Information does not include publicly available information

❖ ***Business*** is defined as any for-profit legal entity doing business in Pennsylvania that collects consumers' personal information "or on the behalf of which such information is collected" and determines the purposes and means of processing of consumers' financial information that meets one of these thresholds:

- Annual Gross Revenue greater than $10 million
- Alone or in combination, buys, receives for a commercial purpose, sells for a commercial purpose the personal information of 50,000+ consumers, households, or devices or
- Derives 50% or more of annual revenues from selling consumers' personal information.

❖ ***Business*** also includes any entity that controls a business as defined above and shares common branding with the business.

Enforcement

❖ The Attorney General may bring a civil action to recover penalties

- ***Private Right of Action***
  - A consumer may bring a civil action for damages of no less than $100 and no more than $750 per consumer per incident and may seek injunctive or declaratory relief.

Data Safe Harbors

- A business or service provider is not required to comply with a consumer's request to delete information if it is necessary for the business/service provider to maintain the consumer's personal information to:
  - Complete the transaction for which the information was collected
  - Detect security incidents
  - To identify and repair errors that impair functionality
  - Exercise free speech
  - Engage in public or peer-reviewed research
  - To enable internal uses that are aligned with the expectations of the consumer
- This law will not restrict a business's ability to comply with the law; civil/criminal/or regulatory inquiry; cooperate with law enforcement; exercise/defend legal claims; collect/use/retain/sell or otherwise disclose de-identified data; or collect or sell a consumer's personal information if every aspect of the commercial conduct occurs outside Pennsylvania.

Vendor Provisions

- A third party shall not sell personal information about a consumer that was sold to the third party by a business unless the consumer received explicit notice and provided an opportunity to opt out.

Pennsylvania

Consumer Data Privacy Act

- Legislative Status: Referred to Consumer Affairs; April 7, 2021.
- Link to Text: HB 1126

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared		✓
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Business*** means either:
  - A for-profit legal entity
    - That is organized or operated for the profit or financial benefit of its shareholders or other owners.
    - That collects consumers' personal information, or on behalf of which consumers' personal information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information.
    - That does business in this commonwealth.
    - That satisfies one or more of the following thresholds:
      - Has annual gross revenues in excess of $10 million.

- Alone or in combination, annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices.

- Derives 50% or more of annual revenues from selling consumers' personal information.

➢ An entity that controls a business under paragraph (1) and shares common branding with the business.

❖ ***Personal information*** means information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household, including:

➢ Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, including an internet website protocol address, e-mail address, account name, Social Security number, driver's license number, passport number or other similar identifiers.

➢ Characteristics of protected classifications under federal or state law.

➢ Commercial information, including records of personal property, products or services purchased, obtained or considered or other purchasing or consuming histories or tendencies.

➢ Biometric information.

➢ Internet or other electronic network activity information, including browser history, search history and information regarding a consumer's interaction with an internet website, application or advertisement.

➢ Geolocation data.

➢ Audio, electronic, visual, thermal, olfactory or similar information.

➢ Professional or employment-related information.

- Education information, defined as information that is not publicly available personally identifiable information under the Family Educational Rights and Privacy Act of 1974 (Public Law 90-247, 20 U.S.C. §1232g).

- Inferences drawn from any of the information identified under this definition to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviors, attitudes, intelligence, abilities and aptitudes.

❖ Personal information does not include publicly available information.

Enforcement

❖ ***Attorney General***

- The Attorney General may enforce through civil actions and penalties.

❖ ***Private Right of Action***

- A consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

  - To recover damages in an amount not less than $100 and not more than $750 per consumer per incident or actual damages, whichever is greater.

  - Injunctive or declaratory relief.

  - Any other relief the court deems appropriate.

Safe Harbors

❖ To complete a transaction for which the personal information was collected, provide a good or service requested by the consumer or reasonably anticipated within the context

of the businesses' ongoing business relationship with the consumer or otherwise perform a contract between the business and consumer;

- Detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Exercise free speech;
- Engage in certain public or peer-reviewed scientific, historical or statistical research;
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- Compliance with legal obligations.

Vendor

- A third party may not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out.
- A business that receives a verifiable request from a consumer to delete the consumer's personal information shall delete the consumer's personal information from its records and direct service providers to delete the consumer's personal information from the service provider's records.

Texas

Personal Identifying Information Processed or Collected by Certain Businesses

- Legislative Status: Referred to Business & Industry Committee
- Link to Text: HB 3741
- Effective Date: September 1, 2021[24]

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared[25]		✓
Right to Correction	✓	
Right to Deletion[26]	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out		✓
Opt In[27]	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Personal Identifying Information*** means a category of information relating to an identified or identifiable individual. This includes:
  - Social Security number, driver's license number, passport number, military identification number, or any other similar number issued on a government document and used to verify an individual's identity;
  - Financial account number, credit or debit card number, or any security code, access code, or password that is necessary to permit access to an individual's financial account;

[24] Sections 541.054 and 541.155 would take effect January 1, 2022.
[25] Right to the names of third parties to which information has been distributed, transferred, or sold by the business.
[26] Right to delete sensitive personal information. § 541.054
[27] Required for performing geolocation tracking or to sell information related to such tracking.

- Physical or mental health information (including health care information);
- Unique biometric information (fingerprint, voice print, retina or iris image, etc.)
- Religious affiliation or practice information;
- Racial or ethnic origin information;
- Precise geolocation tracking data; and
- Unique genetic information

❖ ***Personal Identifying Information*** does <u>not</u> include a specific category of personal identifying information that the Attorney General exempts from this definition by rule.

❖ ***Category one information*** means personal identifying information that an individual must use in personal, civic, or business setting, and includes:

- Social Security numbers, driver's license numbers, passport numbers, military identification numbers, or any similar number issued on a government document and used to verify an individual's identity;
- Financial account numbers, credit or debit card numbers, any security code, access code, or password that is necessary to permit access to an individual's financial account;
- Unique biometric information, including a fingerprint, voice print, retina or iris image, or any other unique physical representation; and
- The private communications or other user-created content of an individual that is not publicly available.
- Physical or mental health information, including health care information; and

❖ ***Category two information*** means personal identifying information that may present a privacy risk to an individual, including members of a constitutionally protected class, and includes:

- Racial or ethnic information;
- Religious affiliation or practice information;
- Age;
- Physical or mental impairment;
- Precise geolocation tracking data; and
- Unique genetic information.

❖ ***Category three information*** means specific facets of personal identifying information and includes:

- Time of birth; and
- Political party or association.

❖ ***Business*** means a for-profit entity, including a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit of financial benefit of the entity's shareholders or other owners.

❖ ***Third party*** means a person engaged by a business to process, on behalf of the business, personal identifying information collected by the business.

Enforcement

❖ The Attorney General may bring actions in the name of the state against the business or third party for:

- Civil penalties of not more than $10,000 per violation — not to exceed $1 million; and
- Reasonable attorneys' fees, court costs, and investigatory costs, incurred in bringing an action under this section.

❖ ***No Private Right of Action***

Data Safe Harbors

- The act applies to a business that:
  - Does business in this state;
  - Has more than 50 employees;
  - Collects the personal identifying information of more than 5,000 individuals, households, or devices or has that information collected on the business's behalf; and
  - Satisfies one or more of the following thresholds:
    - Has annual gross revenue in excess of $25 million; or
    - Derives 50% or more annual revenue by processing personal identifying information.

- This act does not apply to:
  - Nonprofits or governmental entities
  - Publicly available information
  - Protected health information governed by Chapter 181 of the Health and Safety Code
  - Information that is collected by an entity governed under HIPAA
  - Information collected or governed under Title XII of the American Recovery and Reinvestment Act of 2009
  - Personal identifying information collected by a consumer reporting agency, as defined in Tex. Bus. & Comm. Code § 20.01, if the information is used to generate or reported in a consumer report and complying with the Fair Credit Reporting Act and solely used for a purpose authorized under that act

- Personal information collected, processed in accordance with Gramm-Leach-Bliley Act (GLBA) of 1999 and its regulations

- Education information that is not publicly available personally identifiable information under the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g) (34. C.F.R. Part 99);

Vendor Provisions

- A business that discloses to a third party to process on behalf of the business is not liable for a third party's violation of Section 541.155(b) if the business does not have actual knowledge or a reasonable belief that the third party intend to violate that section.

- A business may not sell, transfer, or communicate category two information to any third party.

Utah

Consumer Privacy Act

- Legislative Status: Senate File for Bills Not Passed
- Link to Text: S.B. 249

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out	✓	
Children		✓
Data Destruction		✓

Key Definitions

- ***Advertiser*** means a person that advertises the person's product, service, or website through the use of commercial email.

- ***Collector*** means for-profit legal entity that:

  - Collects personal information from consumers; and

  - (i) Has annual gross revenue of more than $25 million; (ii) alone or in combination with wholly owned subsidiaries, buys, receives for the entity's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more residents of this state; or (iii) derives 50% or more of the entity's annual revenue from selling personal information from consumer.

- ***Consumer*** means a natural person.

- ***Personal information*** means:

- Any information that directly identifies an individual;
- Any representation of information that permits the direct or indirect identification of the individual to whom the information applies; or
- Any information that permits physical or online contact with a specific individual.
- "Personal information" includes: (i) a name; (ii) an address; (iii) a Social Security number or other identifying number or code; (iv) a telephone number; and (v) an email address.

Enforcement

- ***Attorney General and Private Right of Action***
  - The Office of the Attorney General or a consumer may bring a claim against a collector that violates this section to recover: (a) actual damages to the consumer; (b) except as provided in Subsection (2), liquidated damages of $1,000 for each violation; and (c) if the Office of the Attorney General or the consumer is the prevailing party, reasonable attorney fees and costs.

Data Safe Harbors

- A collector is not required to comply with a consumer's request to delete the consumer's personal information if the collector needs to retain the personal information to:
  - Complete the transaction for which the collector collects the personal information;
  - Fulfill the terms of a written warranty or perform a contract between the collector and the consumer;
  - Conduct a product recall in accordance with federal law;
  - Provide a good or a service requested by the consumer or reasonably anticipated within the context of the collector's ongoing business relationship with the consumer detect security incidents;

- Protect against malicious, deceptive, fraudulent, or illegal activity or prosecute an individual responsible for malicious, deceptive, fraudulent, or illegal activity;
- Engage in public or peer-reviewed scientific, historic, or statistical research in the public interest if: (A) deletion of the personal information is likely to seriously impair or make impossible the completion of the scientific, historic, or statistical research; and (B) the consumer provides informed consent;
- Comply with a legal obligation; or
- For consumer provided personal information, use the consumer's personal information internally and in a lawful manner compatible with the context in which the consumer provided the information.

Vendor Provisions

- Consumer may make a consumer request that a collector disclose to the consumer:
  - The categories of personal information that the collector has collected or obtained from a third party;
  - The specific personal information that the collector has collected or obtained from a third party regarding the consumer;
  - The source of the information described in Subsection (2)(a)(ii); or
  - Any third party to which the collector disclosed the consumer's personal information.

Utah

Consumer Privacy Act

- Legislative Status: Senate file for bills not passed.
- Link to Text: S.B. 200

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction		✓
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means an individual who is a resident of the state acting in an individual or household context. Consumer does not include an individual acting in an employment or commercial context.

- ***Controller*** means a person doing business in the state who determines the purposes for which and the means by which personal data is processed, regardless of whether the person makes the determination alone or with others.

- ***Covered entity*** means the same as that term is defined in 45 C.F.R. Sec. 160.103.

- ***Personal data*** means any information that: (i) identifies or describes an identifiable individual; or (ii) is reasonably capable of identifying or describing an identifiable individual. "Personal data" does not include de-identified data, anonymous or pseudonymous data, or publicly available information.

- ***Processor*** means a person who processes personal data on behalf of a controller.

- ***Sensitive data*** means: (i) personal data that reveals an individual's: (A) racial or ethnic origin; (B) religious beliefs; (C) diagnosed mental or physical health condition; (D) sexual orientation; or (E) citizenship or immigration status; (ii) the processing of genetic or biometric personal data for the purpose of identifying an individual; (iii) the personal data of a known child; or (iv) specific geolocation data. "Sensitive data" does not include personal data that reveals an individual's racial or ethnic origin, if the personal data is processed by a video communication service.

Enforcement

- ***Attorney General***
  - The Attorney General may take enforcement action against violators and impose penalties for violation.
- ***Private Right of Action***
  - Creates a cause of action for the Office of the Attorney General, the electronic mail service provider, the recipient of the unsolicited commercial email, and any person whose brand, trademark, email address, or domain name is used without permission to recover damages related to unauthorized or misleading commercial email.

Data Safe Harbors

- ✓ Compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by a federal, state, local or other governmental entity.
- ✓ Cooperation with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
- ✓ Investigation, establishment, exercises, preparation for or defense of a legal claim;
- ✓ Providing a product or service requested by a consumer;

- ✓ Performance of a contract to which the consumer is a party, or taking steps at the request of the consumer before entering into a contract with the consumer;
- ✓ Taking immediate steps to protect an interest essential for the life or physical safety of the consumer or of another individual;
- ✓ Detection and responses to certain security incidents;
- ✓ Preservation of the integrity of security systems, books, and records;
- ✓ Engagement in certain public or peer-reviewed scientific, historical, or statistical research in the public interest;
- ✓ To assist with an obligation in this Act;
- ✓ Where compliance would violate an evidentiary privilege of Utah law;
- ✓ Where compliance would adversely affect the rights of any person;
- ✓ Where compliance would violate a privileged communication.

Vendor Provisions

- ❖ A processor shall only engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

Virginia

Personal Data; Management and Oversight

- Legislative Status: Continued to 2021
- Link to Text: HB 473

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability		✓
Privacy Notice Required	✓	
Opt Out		✓
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is a resident of the commonwealth acting only in an individual or household context.

  Consumer does not include a natural person acting in a commercial or employment context.

- ***Personal Data*** means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

- ***Business*** is not defined by the bill. However, it defines the jurisdictional scope of the bill as applicable to legal entities (i) that conduct business in the commonwealth or produce products or services that are intentionally targeted to residents of the commonwealth and (ii) that:

  - Control or process personal data of 100,000 consumers or more; or

- Derive over 50% of gross revenue from the sale of personal data and process or control personal data of 25,000 consumers or more

Controller means the person that, alone or jointly with others, determines the purposes and means of the processing of personal data.

Enforcement

- Any violation shall constitute a prohibited practice pursuant to the Virginia Consumer Protection Act and shall be subject to any and all enforcement provisions therein.

- Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

Data Safe Harbors

- The obligations imposed on controllers under this chapter do not restrict a controller's ability to:

  - Comply with federal, state or local laws, rules or regulations

  - Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, local or other governmental authorities

  - Cooperate with law-enforcement agencies

  - Investigate, exercise or defend legal claims

  - Prevent or detect identity theft, fraud or other criminal activity or verify identities

  - Enter into a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract

  - Protect the vital interests of the consumer or of another individual

- Perform a task carried out in the public interest or in the exercise of official authority vested in the controller

- Process personal data of a consumer for one or more specific purposes where the consumer has consented in writing to the processing; or

- Prevent, detect or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report or prosecute those responsible for any such action

Vendor Provisions

- Third parties must honor objection requests received from third-party controllers.

Virginia

Consumer Data Protection Act (CDPA)

- Legislative Status: Passed into law March 2, 2021
- Link to Text: H2307
- Effective Date: 01/01/2023

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is a resident of the commonwealth acting only in an individual or household context.

  Consumer does not include a natural person acting in a commercial or employment context.

- ***Personal Data*** means any information that is linked or reasonably associated to an identified or identifiable natural person.

- ***Personal Data*** does not include de-identified data or publicly available information.

- ***Sensitive Data*** means a category of personal data that includes:

  - Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

- The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- The personal data collected from a known child; or
- Precise geolocation data.

- ***Business*** is not defined by the bill. However, it defines the jurisdictional scope of the bill as applicable to legal entities (i) that conduct business in the commonwealth or produce products or services that are intentionally targeted to residents of the commonwealth and (ii) that:
  - Control or process personal data of 100,000 consumers or more; or
  - Derive over 50% of gross revenue from the sale of personal data and process or control personal data of 25,000 consumers or more

  Controller means the natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data.

Enforcement

- Only the Attorney General may enforce this chapter.
- The Attorney General shall provide written notice of any alleged violation, and the controller or processor has 30 days to cure and notify of cure without penalty.
- Violations may result in civil penalties of up to $7,500 per violation, injunctions, and reasonable expenses including attorney fees.

Data Safe Harbors

- A controller, processor, or third party in compliance with this chapter is not liable for a violation involving shared personal information by another controller, processor, or third party unless it actually knew of the intent to violate this chapter
- This bill does not apply to:

- Persons or entities that do not control or process personal data of at least
  - (1) 100,000 consumers; or
  - (2) 25,000 consumers and derive over 50% of gross revenue from the sale of personal data
- Any body, authority, board, bureau, commission, district, or agency of the commonwealth or of any political subdivision of the commonwealth
- Financial institutions or data subject to Title V of the Gramm-Leach-Bliley Act
- Entities or business associates governed by the privacy, security, and breach notification rules issued by the Department of Health and Human Services under C.F.R. Parts 160 and 164
- Nonprofit organizations
- Institutions of higher learning
- Information that meets the definition of:
  - Protected health information under HIPAA
  - Health records for the purposes of Title 32.1
  - Patient identifying information for the purposes of 42 U.S.C. § 290dd-2
  - Identifiable private information under 45 C.F.R. Part 46
  - Identifiable private information collected as part of human subjects research and meeting the guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use
  - 21 C.F.R. Parts 6, 50, and 56 used to protect human subjects

- Personal data used or shared in research in accordance with this chapter or other research conducted in accordance with applicable law
- Patient safety work product for the purposes of the federal Patient Safety and Quality Improvement Act
- De-identified information as defined in HIPAA

- Information created for purposes of the federal Health Care Quality Improvement Act of 1986
- The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated and authorized under the federal Fair Credit Reporting Act
- Information originating from, and intermingled as to become indistinguishable with, or information treated in the same manner as information exempt under this subsection that is (1) maintained by a covered entity or business associate under HIPAA; or (2) a program or service organization under 42 U.S.C. § 290dd-2
- Information used only for public health activities and purposes as authorized under HIPAA
- Information used in compliance with
  - The federal Farm Credit Act
  - The federal Driver's Privacy Protection Act
- Information regulated by the Federal Family Educational Rights and Privacy Act
- Data processed or maintained (1) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party so long as the information is collected and used for that

context; (2) as emergency contact information for emergency contact purposes; and (3) in administration of employee benefits for a beneficiary

- The obligations imposed on controllers under this chapter do not restrict a controller, processor, or third party's ability to:
  - Comply with federal, state or local laws, rules or regulations
  - Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, local or other governmental authorities
  - Cooperate with law enforcement agencies based on reasonable and good faith belief that conduct or activity violates the law, rules, or regulations
  - Investigate, exercise or defend legal claims
  - Prevent, detect or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report or prosecute those responsible for any such action
  - Enter into a contract to which the consumer is a party, including fulfilling the terms of a written warranty; take steps at the request of the consumer prior to entering into a contract; or provide a product or service as requested by the consumer
  - Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis
  - Assist another controller, processor, or third party with any of the obligations under this subsection
  - Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the

controller; (ii) the expected benefits of the research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification

- Conduct internal research to develop, improve, or repair products, services, or technology
- Identify and repair technical errors that impair existing or intended functionality
- Effectuate a product recall
- Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically request by a consumer or the performance of a contract to which the consumer is a party
- Comply with evidentiary privilege rules under the commonwealth

Vendor Provisions

- The contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller, and it shall:
  - Set forth:
    - Instructions for processing data;
    - The nature and purpose of processing;
    - The type of data subject to processing;
    - The duration of processing; and
    - The rights and obligations of both parties;
  - Include requirements that:

- Each person processing is subject to a duty of confidentiality with respect to the data;
- At the controller's direction, the processor shall delete or return all personal data to the controller as requested at the completion of the provision of services, unless retention is required by law;
- Upon reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations of this chapter; and
- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and
- Engage any subcontractor pursuant to a written contract that (1) requires the subcontractor to meet the obligations of the processor with respect to personal data; and (2) does not purport to relieve any party from liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

❖ The controller in possession of de-identified data shall contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

❖ A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirement of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter provided that, at the time of disclosing the personal data, the disclosing party did not have actual knowledge that the recipient intended to commit a violation.

❖ A third-party controller or processor that receives personal data from a controller or processor in compliance with this chapter is not in violation of this chapter for the transgressions of the controller or processor from which it receives personal data.

Washington

Washington Privacy Act

- Legislative Status: Died in Committee.
- Link to Text: SB 5062
- Effective Date: July 31, 2022[28]

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- ***Consumer*** means a natural person who is a Washington state resident acting only in an individual or household context.

  Consumer does not include a natural person acting in a commercial or employment context.

- ***Consent*** means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose.

  Consent is not acceptance of general or broad terms or a similar document that contains descriptions of personal data processing along with other, unrelated information. Hovering over, muting, pausing, or closing a given piece of content is not consent. An agreement obtained through dark patterns is not consent.

[28] Sections 101-118 do not apply to nonprofits or higher education institutions until July 31, 2026. Parts 2-3 are effective immediately, but those are specific to contact tracing and are not covered in this summary. Please see last page of this section.

- ***Dark pattern*** means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

- ***Personal Data*** means any information that is linked or reasonably linkable to an identified or identifiable natural person.

  Personal Data does not include de-identified data or publicly available information (information that is lawfully made available from federal, state or local government records.)

- ***Business*** is not defined by the bill. However, it defines the jurisdictional scope of the bill as applicable to legal entities that conduct business in Washington, or produce products or services that are intentionally targeted to residents of Washington and that satisfy one or more of the following thresholds:

  - Controls or processes personal data of 100,000 consumers or more

  - Derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more

- ***Controller*** is a natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- ***Processor*** is a natural or legal person that processes personal data on behalf of the controller. Processing is governed by a contract between the controller and the processor that sets out the processing instructions to which the processor is bound.

Enforcement

- The Washington Attorney General may bring an action under the consumer protection act RCW 19.86 for civil penalties of up to $7,500 per violation, reasonable attorney fees, and investigation costs.

- The Attorney General, prior to filing a complaint, must provide a warning letter, and may only bring an action if after 30 days the Attorney General believes the alleged violations are not cured.

❖ ***Private Right of Action***

- A consumer alleging a violation of this act's consumer rights (§ 103) or prohibitions against discrimination on the basis of protected class (§ 107(6)), processing sensitive data (§107 (8)), or processing a minor's personal data for targeted advertising or sale (§ 107(9)), may bring a civil action seeking appropriate injunctive relief and reasonable attorney fees and costs.

Data Safe Harbors

❖ The bill does not apply to:

- State and local governments
- Municipal corporations
- Air carriers
- Nonprofit organizations that
  - Are registered with the Secretary of State under the charities program pursuant to chapter 19.09 RCW;
  - Collect personal data during legitimate activities related to the organization's tax exempt purpose; and
  - Do not sell personal data collected by the organization
- Information that meets the definition of[29]:
  - Protected Health Information under HIPAA
  - Health care information for purposes of 70.02 RCW

[29] The limitations set forth in this bullet point also apply to information maintained by a covered entity or business associate as defined by HIPAA; a health care facility or health care provider as defined by RCW 70.02.010; or a program or qualified service organization as defined by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290 dd-2.

- Patient identifying information for purposes of 42 C.F.R. Part 2
- Identifiable private information for purposes of the Federal Policy for the Protection of Human Subjects
- Information and documents created specifically for, and collected and maintained by: a quality improvement committee, a peer review committee, a quality assurance committee, a hospital for reporting of health care-associated infections, a notification of an incident or reports regarding adverse events
- Information and documents created for purposes of the Federal Health Care Quality Improvement Act of 1986, and related regulations; or
- Patient safety work product information for purposes of 42 C.F.R. Part 3

➢ Information originating from, and intermingled to be indistinguishable with, information under the previous point that is maintained by and entity regulated under HIPAA or RCW 70.02.10 or a program or qualified service organization under 72 C.F.R. Part 2

➢ Information used only for public health activities and purposes described in 45 C.F.R. § 164.512 or collected and maintained under the Washington Health Benefit Exchange in RCW 43.71

➢ Personal data provided to, from or held by a consumer reporting agency where such use is in compliance with the federal Fair Credit Reporting Act

➢ Personal data collected, processed, sold or disclosed pursuant to the GLBA

➢ Personal data collected, processed, sold or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994 or the federal Farm Credit Act of 1971, where such use is in compliance with the law

➢ Personal data regulated by the federal Family Education Rights and Privacy Act or the Student User Privacy in Education Rights Act

- Information maintained for emergency contact, job applicant, employment records, or benefit administration purposes

❖ The obligations set forth in the bill do not restrict a controller's or processor's ability to:

- Comply with federal, state or local laws, rules, or regulations
- Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, local or other governmental authorities
- Cooperate with law enforcement agencies
- Investigate, exercise or defend legal claims
- Prevent or detect identity theft, fraud or other criminal activity or verify identities
- Provide a product or service specifically requested by a consumer, or perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract
- Protect the essential interests for the life of the consumer or of another natural person where the processing cannot be manifestly based on another legal basis
- Perform a task carried out in the public interest (public or peer-reviewed scientific, historical, or statistical research) if an independent oversight entity concludes (i) it is likely to provide substantial benefits that do not exclusively accrue to the controller, (ii) the expected benefits outweigh the risks, and (iii) the controller has implemented reasonable safeguards to mitigate the privacy risks — including those associated with re-identification
- Assist another controller, processor, or third party with any of the obligations under this subsection
- Prevent, detect or respond to security incidents or investigate, report or prosecute those responsible for any such action
- Retain, use, or collect data to

- Identify and repair technical errors that impair existing or intended functionality; or

- Perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with the processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party when those internal operations are performed during, and not following, the consumer's relationship with the controller

Vendor Provisions

- A disclosing controller or processor in compliance with this chapter is not liable for the violations of a recipient controller or processor provider the disclosing party did not have actual knowledge that the recipient intended to commit a violation at the time of disclosure.

- A receiving controller or processor in compliance with this chapter is not liable for the violations of a disclosing processor or controller.

- Processors are responsible for adhering to the controller's instructions and assisting the controller to meet its obligations under this chapter.

- The contract between the controller and processor governs processing, and it must:

  - Set out:

    - The nature and purpose of the processing;

    - The type of personal data subject to the processing;

    - The duration of the processing; and

    - The obligations and rights of both parties.

  - Require:

- Ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data;
- Engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with the provisions controller the controller-processor contract;
- At the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention is required by law;
- The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and
- The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, and audit of the processor's policies and technical organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable, and provide a report of the audit to the controller upon request.

o Not purport to relieve a controller or processor from liabilities under this chapter.

Special Section

❖ Part 2 creates separate requirements and rights regarding Data Privacy Regarding Public Health Emergency for the Private Sector.

❖ Part 3 creates separate requirements and rights regarding Data Privacy Regarding Public Health Emergency for the Public Sector.

- Parts 2 & 3 become effective immediately and expire June 30, 2024.

Washington

The People's Privacy Act

- Legislative Status: Died in Committee.
- Link to Text: HB 1433

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Annual Opt In	✓	
Children	✓	
Data Destruction[30]	✓	
Right to not be Surreptitiously Surveilled	✓	

Key Definitions

- ***Consent*** is not defined within the definitions section, but it means "freely given, specific, informed, and unambiguous opt-in consent from an individual."

- ***Individual*** means a natural person who is a Washington state resident. Location within the state creates a presumption of residency.

- ***Personal Information*** means any information that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device. Information is reasonably linkable to an individual, household, or device if it can be used on its own or in combination with other information to identify an individual, household, or device.

[30] Yes, where captured personal information (1) was used in violation of this chapter; or (2) is biometric information held for 1 year.

- ***Biometric Information*** is a record of one or more measurable biological or behavioral characteristics that can be used along or in combination with each other or with other information for automated recognition of a known or unknown individual.

- ***Biometric Information*** does not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, physical descriptions (such as height, weight, hair color, or eye color), certain donated organs (including tissue, parts, blood, or serum), health information covered under HIPAA, or scans used to diagnose or treat medical conditions or validate scientific tests.

- ***Captured Personal Information*** is personal information captured in an interaction in which a covered entity directly or indirectly makes available information, products, or services to an individual or household.

  - This includes targeted ads, offering membership, posting of a product or service, or posting information.

  - All biometric information, regardless of how captured, is included.

  - De-identified captured personal information must still be safeguarded, and, if shared, the covered entity must contractually obligate recipients to comply with these provisions and submit to the jurisdiction.

- ***Covered Entity*** means a person or legal entity that is not a governmental entity and that conducts business in Washington state, processes captured personal information, and:

  - Has earned or received $10 million or more of annual revenue through 300 or more transactions; or

  - Processes and/or maintains the captured personal information of more than 1,000 unique individuals during the course of a calendar year.

- ***Washington governmental entity*** means a department or agency of Washington state or a political subdivision thereof, including but not limited to public authorities and special use districts, or an individual acting for or on behalf of the state or a political subdivision thereof.

- ***Processing*** means any action or set of actions performed on or with personal information.
  - This includes collecting, sharing, accessing, using, storing, transmitting, etc.
  - Processing is governed by a contract between the covered entity and the data processor that prohibits processing captured personal information except as authorized by contract and this bill.
- ***Processing*** does not include these same actions listed above where captured personal information is encrypted as to be inaccessible to the person or entity.
- **Harm** means "potential or realized adverse consequences to an individual or society . . ."

Enforcement

- The Washington Attorney General may bring an action either in the name of the state, or as *parens patriae* on behalf of persons residing in the state, to enforce this chapter.
- City attorneys or county prosecutors with populations over 200,000 may bring an action.
- Any of the parties above may seek:
  - Up to $25,000 per violation or 4% of the defendant's annual revenue (whichever is greater);
  - Injunctive relief, including preliminary injunctions;
  - Other appropriate relief, including restitution, to redress harms to individuals or to mitigate all substantial risk of harm; and
  - Any other relief the court deems appropriate.
- ***Private Right of Action***
  - Any individual that alleges a violation may bring a civil action for liquidated damages of $10,000 or actual damages, whichever is greater; punitive damages;

reasonable attorneys' fees and costs; and any other relief the court deems appropriate, including but not limited to an injunction.

Data Safe Harbors

- Aspects of the bill do not apply to Washington governmental entities.
- Nothing in this chapter shall diminish any individual's or entity's rights or obligations under 70.02 RCW.
- The bill does not apply to:
  - Information in the public domain, such as a name and address available on a publicly recorded deed
  - Individuals sharing their personal contact information with other individuals in the workplace, social, political or similar settings where the purpose of the information is to facilitate communication among such individuals; however, processing this information beyond interpersonal communication is covered by this chapter
  - Biometric information collected, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, insurance, payment, or operations under HIPAA
  - Scans and filming[31] of human anatomy used exclusively to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening
  - Information that meets the definition of health care information captured from a patient by a provider or facility as defined in RCW 48.41.030
- Section 9(1): Regarding captured personal information, a covered entity or Washington governmental entity shall not be required to obtain freely given, specific, informed, and unambiguous opt-in consent under section 5(2) or 7(1) if

[31] Includes X-ray roentgen process, computed tomography, MRIs, PET scans, mammographies, and "other image or film of human anatomy."

- (1) It is processing only de-identified information

- (2) It believes an emergency involving immediate danger of death or serious physical injury to an individual requires obtaining without delay captured personal information related to the emergency; and (2) the request is narrowly tailored to address the emergency. This is subject to the following limitations:

    - The request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to an individual requires obtaining without delay captured personal information relating to the emergency; and

    - Simultaneously with obtaining the captured personal information, the entity shall use reasonable efforts to inform the individual of the captured personal information obtained; the details of the emergency; and the reasons why the entity needed to use, access, or disclose the biometric information and shall continue such effort to inform until the receipt of information is confirmed

- (3) Disclosure is required to respond to a warrant or subpoena issued by a court of competent jurisdiction or a subpoena issued by a governmental entity or pursuant to a pending judicial proceeding:

    - (i) Unless a delayed notice is ordered, both the entity requesting the warrant or subpoena and any entity receiving such warrant or subpoena shall, simultaneous with requesting or receiving a warrant compelling disclosure of or serving or receiving a subpoena for captured personal information, serve or deliver the following information to the subject of warrant or subpoena by registered or first-class mail, email, or other means reasonably calculated to be effective:

        - A copy of the warrant or subpoena and notice that informs the individual of the nature of the inquiry with reasonable specificity;

        - That captured personal information maintained for the individual was supplied to or requested by the requesting entity and the date on which the supplying or request took place;

- An inventory of the captured personal information requested or supplied; and
- The identity of the entity or individual from which the information is requested

- (ii) A covered entity or Washington governmental entity processing only de-identified information[32] may apply to the court for an order delaying notification, and the court may issue the order if the court determines that there is reason to believe that notification of the existence of the warrant will result in endangering the life or physical safety of an individual, flight from prosecution, destruction or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

- (iii) A covered entity subject to a subpoena shall postpone compliance until it has given the subject of the subpoena notice of the information required under this subsection (2)(b)(i) and has allowed at least 10 business days for the subject to seek review of or otherwise challenge the subpoena

❖ The consumer's right to deletion does not apply to the extent:

➢ Retention is required under existing laws or regulation; or

➢ The information is exempt from consent as mentioned above (section 9(1))

Vendor Provisions

❖ A covered entity shall not disclose captured personal information to a third party unless that third party is contractually bound to the covered entity to meet the same privacy and security obligations as the covered entity.

❖ A covered entity shall exercise reasonable oversight and take reasonable actions, including auditing the data security and processing practices of third parties it provides captured personal information to at least once annually and ensures the third party's

[32] The actual text of the bill references this as part (d) of this subsection.

compliance with such contractual provisions. The covered entity shall publish the results of the audit publicly on its website.

- A covered entity shall not disclose captured personal information to a data processor unless the covered entity enters into a contractual agreement with the data processor that:
  - Requires the data processor to meet the same privacy and security obligations as the covered entity; and
  - Prohibits:
    - The data processor from processing the captured personal information for any purpose other than the purpose for which the individual provided the captured personal information to the covered entity; and
    - The data processor from further disclosing or processing captured persona information it has acquired from the covered entity except as explicitly authorized by the contract and consistent with this chapter.
- A covered entity shall exercise reasonable oversight and take reasonable actions, including auditing the data security and processing practices of the data processor at least once annually and ensure the data processor's compliance with such contractual provisions. The covered entity shall publish the results of the audit publicly on its website.
- If a covered entity that has facilitated access to captured personal information by other entities has knowledge that an entity to which captured personal information was provided is using such data in violation of this chapter, then the covered entity shall immediately limit the violator's access to such captured personal information and seek proof of destruction of such captured personal information by the violating entity.

West Virginia

Consumer Data Privacy

- Legislative Status: Introduced in House on 03/15/21
- Link to Text: HB 3159

Consumer Rights	Yes	No
Access to Personal Information Collected	✓	
Access to Personal Information Shared	✓	
Right to Correction	✓	
Right to Deletion	✓	
Right to Data Portability	✓	
Privacy Notice Required	✓	
Opt Out	✓	
Children	✓	
Data Destruction		✓

Key Definitions

- Business means either:
  - A for-profit legal entity that
    - Does business in this state;
    - Collects personal information about consumers, or is the entity on behalf of which such information is collected;
    - Determines the purposes and means of processing personal information about consumers alone or jointly with others; and
    - Satisfies one or more of the following thresholds:

- (i) Has global annual gross revenues in excess of $25 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

- (ii) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices.

- (iii) Derives 50% or more of its global annual revenues from selling or sharing personal information about consumers.

➢ Any entity that controls or is controlled by a business and that shares common branding with the business.

❖ ***Consumer*** means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, and who is:

➢ In this state for other than a temporary or transitory purpose; or

➢ Domiciled in this state but resides outside this state for a temporary or transitory purpose.

❖ ***Personal information*** means information that identifies, relates to, or describes a particular consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer or household, including;

➢ Identifiers such as a real name, alias, postal address, unique identifier, online identifier, internet protocol address, email address, account name, Social Security number, driver license number, passport number, or other similar identifiers.

➢ Information that identifies, relates to, or describes, or could be associated with, a particular individual, including, but not limited to, a name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

- Characteristics of protected classifications under state or federal law.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information that is not publicly available, personally identifiable information as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.
- Inferences drawn from any of the information identified in this paragraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

❖ ***Personal information*** does not include consumer information that is:

- Publicly and lawfully made available from federal, state, or local government records.
- De-identified or aggregate consumer information.

❖ ***Service provider*** means a for-profit legal entity, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal

information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this section, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

Enforcement

- West Virginia Division of Consumer Protection
  - If the West Virginia Division of Consumer Protection has reason to believe that any business, service provider, or other person or entity is in violation of this article and that proceedings would be in the public interest, the division may bring an action against such business, service provider, or other person or entity and may seek a civil penalty of not more than $2,500 for each unintentional violation or $7,500 for each intentional violation. Such fines may be tripled if the violation involves a consumer who is 16 years of age or younger.
  - Division may adopt rules to implement the article.
- ***Private Right of Action***
  - A consumer whose nonencrypted and nonredacted personal information or e-mail address, in combination with a password or security question and answer that would allow access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may bring civil action for any of the following:
    - (1) Damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.
    - (2) Injunctive or declaratory relief, as the court deems proper.

Data Safe Harbors

- A business does not sell personal information when: The service provider does not further collect, sell, share, or use the personal information of the consumer except as necessary to perform the business purpose.

- A business or a service provider may not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information to do any of the following:

  - Complete the transaction for which the personal information was collected.

  - Fulfill the terms of a written warranty or product recall conducted in accordance with federal law.

  - Provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

  - Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

  - Debug to identify and repair errors that impair existing intended functionality.

  - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

  - Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

  - Comply with a legal obligation.

- Otherwise internally use the consumer's personal information in a lawful manner that is compatible with the context in which the consumer provided the information.

Vendor Provisions

- Any contract between a business and a service provider must prohibit the service provider from:
  - Selling or sharing the personal information;
  - Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business;
  - Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business; or
  - Combining the personal information that the service provider receives from or on behalf of the business with personal information that it receives from or on behalf of another person or entity or that the service provider collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose.
- Any contract between a business and a third party must prohibit the third party that receives a consumer's personal information from the following:
  - Selling or sharing the personal information.
  - Retaining, using, or disclosing the personal information for any purpose other than the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
  - Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

- The contract must include a certification made by the person or entity receiving the personal information stating that the person or entity understands and will comply with the restrictions under this article.

- Any contract between a business and a third party or between a business and a service provider for receiving personal information must include a provision that any contract between a third party and any subcontractor or between a service provider and any subcontractor must require the subcontractor to meet the obligations of the third party or service provider with respect to personal information.

