
State Comprehensive Privacy Law Update for 2022

JANUARY 28, 2022

As companies prepare for new privacy laws to go into effect in California, Virginia, and Colorado, they should also keep an eye out on other states that are looking to pass their own “comprehensive” privacy legislation. Legislatures may be more motivated to pass privacy bills this time around now that two other states have joined California. There are also several states (such as Florida, Washington, and New York) that are trying to pass the same bills as have been proposed in prior years and hoping to have more success this time around.

We have summarized the most important comprehensive privacy bills being considered at the state level, as well as the key trends identified in these bills overall. Please let us know if you have questions about these bills or if any questions arise as these proposals move forward.

Key Trends and Highlights

1. The bills being considered at the state level are similar in many ways. For example, they all only apply to businesses that meet a certain data processing or revenue threshold within a state (similar to the original CCPA—although the levels are different in every state). They all also require businesses to provide consumers with individual data privacy rights and to comply with data subject access requests.
2. Most of the bills (all except proposals in Indiana and Mississippi) contain exemptions for data that is regulated at the federal level (such as by HIPAA, GLBA, or FERPA)—meaning that these laws often are not actually “comprehensive” privacy laws. However, the exact language of how broad these exemptions apply varies.
3. About half of the bills include additional requirements for the processing of sensitive data or sensitive personal information (similar to the laws in California, Colorado, and Virginia), such as by requiring that entities obtain consumer consent prior to processing such information.
4. The majority of the laws are enforceable by the state attorney general. At least six states (Florida (House bill), Ohio, Mississippi, Kentucky, Pennsylvania, and Washington) create some form of a right to cure, which means that in most cases, an action will not be initiated against the company if it cures the violation.
5. Four states (Florida, New York, Massachusetts, Mississippi) have a proposal with some form of a private right of action. This may be a divisive issue and could lead to these states

not passing privacy legislation. We saw this occur last year with both Florida and Washington.

6. The proposals in Nebraska and the District of Columbia are modeled after the [Uniform Personal Data Protection Act](#), which was adopted by the Uniform Law Commission in 2021.

State Comprehensive Privacy Law Proposals

Florida (Senate bill)

1. *Bill title:* [Florida Privacy Protection Act, S.B. 1864](#)
2. *Current status:* As of January 18, 2022, the bill had been introduced in the Florida Senate and referred to the Commerce and Tourism, Regulated Industries, and Rules committees.
3. *Key provisions:*
 - Applies to “controllers” that either: a) control the processing of personal information of 100,000 or more Florida residents; or b) control or process the personal information of at least 25,000 Florida residents and derive 50% or more of its revenue from selling personal information.
 - Exempts various entities and information types, including covered entities or business associates governed by HIPAA; personal information collected, processed, sold, or disclosed pursuant to GLBA; employee; and B2B information.
 - Creates individual rights for consumers, including the right to opt out of sale through a link on a business’s website that says “Do Not Sell My Personal Information” and the right to opt out of targeted advertising or profiling.
 - Incorporates privacy by design principles, such as purpose limitation and reasonable security practices.
 - Requires consent for the processing of “sensitive data.”
 - Requires businesses to train individuals that handle data subject access requests.
 - Does not create a private right of action. Violations are only enforceable by the Florida AG’s office as unfair or deceptive trade practices.
 - Creates a consumer data privacy unit within the Florida AG’s office.
 - Would go into effect on December 31, 2022.

Florida (House bill)

1. *Bill title:* [H.B. 9](#)
2. *Current status:* As of January 24, 2022, the bill had been introduced in the Florida House and referred to the Commerce Committee.
3. *Key provisions:*
 - Applies to “controllers” that do business in the state, collect consumers’ personal information, determine the purposes and means of processing the information, and that satisfy at least two of the following: a) have global annual revenues over \$50M; b) annually buy, receive, sell, or share the personal information of 50,000 or more

consumers, households, or devices for targeted advertising with third parties or for a purpose other than what has been exempted from the bill; or (c) derive 50 percent or more of global annual revenues from selling or sharing consumers' personal information.

- Exempts various entities and information types, including covered entities or business associates governed by HIPAA and protected health information under HIPAA; covered entities or personal information collected, processed, sold, or disclosed pursuant to the FCRA and GLBA; and information covered by FERPA.
- Requires that controllers maintain an online privacy policy, inform consumers (at or before the point of collection) of the categories of personal information collected and purposes for which the information will be used. Controllers cannot collect additional categories of personal information or use collected information for additional purposes without notice.
- Creates individual rights for consumers, including the right to request a copy of personal data collected, sold, or shared; the right to have personal information deleted or corrected; the right to opt-out of the sale or sharing of personal information through a link on the controller's website that says "Do Not Sell or Share My Personal Information."
- Creates data retention requirements.
- Creates a private right of action for certain claims. Court may award damages between \$100 and \$750 per consumer per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief. Violations are enforceable by the Department of Legal Affairs as an unfair or deceptive trade practice. Delineates situations where penalties can be tripled.
- Gives Florida's Department of Legal Affairs discretion to grant a 45-day cure period for certain violations.
- Would go into effect on July 1, 2023.

Maryland

1. *Bill title:* [Maryland Online Consumer Protection and Child Safety Act, S.B. 11](#)
2. *Current status:* As of January 21, 2022, the bill had been introduced in the Maryland Senate and referred to the Finance Committee.
3. *Key provisions:*
 - Applies to businesses that a) have annual gross revenues over \$25M, b) annually buy, receive, sell, or share personal information of more than 100,000 consumers, households, or devices; or c) derive at least 50% of annual revenues from selling consumers' personal information.
 - Exempts various entities and information types, including health care providers or covered entities governed by HIPAA and information collected by covered entities or businesses associates governed by HIPAA; personal information collected, processed, sold, or disclosed pursuant to GLBA; information covered by FERPA; and employee information.

- Creates individual rights for consumers, including the right to request disclosure of specific pieces of personal information, sources from which information was collected, names of third parties to which the business disclosed the information, and business purposes for third-party disclosure; the right to request deletion of personal information; and the right to opt out of third-party disclosure.
- Does not create a private right of action. Bill authorizes the Maryland AG's office to adopt regulations to carry out the law. A violation of the Act would be an unfair, abusive, or deceptive trade practice.
- Incorporates penalties for unfair trade practices, which includes a civil penalty of up to \$10,000, or up to \$25,000 for a repeat violation. Criminal penalties also apply.
- Would go into effect on January 1, 2023.

New York

1. *Bill title:* [New York Privacy Act, S6701A](#)
2. *Current status:* As of January 23, 2022, the bill had been introduced in the New York Senate and referred to the Consumer Protection Committee.
3. *Key provisions:*
 - Applies to legal persons that conduct business in New York or produce products or services targeted to New York residents and either: a) have annual gross revenue of \$25M or more; b) control or process the personal data of 100,000 or more consumers; c) control or process personal data of 500,000 natural persons or more nationwide and control or process personal data of 10,000 consumers or more; or d) derive over fifty percent of gross revenue from the sale of personal data and control or process personal data of 25,000 consumers or more.
 - Exempts various entities and information types, including information collected by covered entity or business associates governed by HIPAA and the Health Information Technology for Economic and Clinical Health Act; data processed by state and local governments and municipal corporations for processes other than sale; personal data collected, processed, sold, or disclosed pursuant to GLBA; personal data regulated by FERPA; and employee information.
 - Creates individual rights for consumers, including a right to obtain notice of their rights, how they can exercise those rights, and how to withdraw consent; the right to access their personal data as well as information on whether the controller has processed their personal data, and the identity of each processor or third party to whom the controller disclosed, transferred, or sold the consumer's personal data; the right to portable data; the right to have a controller correct inaccurate or incomplete personal data; and the right to have their personal information deleted.
 - Consent is required to process consumers' personal data for certain purposes, and to make changes to existing processing or processing purpose of the personal data that may be less protective of the data than the processing to which consumer has given consent.
 - Incorporates privacy by design principles, such as purpose limitation, and

reasonable safeguards to protect consumer data.

- Requires data protection assessments for activities that present heightened risk of harm.
- Requires data brokers to register, pay an annual fee to the New York AG, and submit information of their data use practices.
- Creates a private right of action. Violations are also enforceable by the New York AG's office.
- The New York AG can bring action to enjoin any violation, to obtain restitution and disgorgement of any money or property obtained by the violation, and to obtain civil penalties of up to \$15,000 per violation.
- Creates penalties for data brokers that fail to register or that submit false information in registration. Creates civil penalty of \$1,000 for each day the data broker fails to register or correct false information, an amount equal to the fees that were due during the period it failed to register, and expenses incurred by the New York AG in the investigation and prosecution of the action.
- Would go into effect immediately, with certain sections taking effect two years after they become law. The private right of action would take effect three years after the section becomes law.

Massachusetts

1. *Bill Title:* [Massachusetts Information Privacy Act, S. 46](#)
2. *Current Status:* As of January 23, 2022, the bill had been introduced in the Massachusetts Senate and referred to the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity.
3. *Key Provisions:*
 - Applies to “covered entity” that conducts business in Massachusetts and that processes personal information by itself or by contracting with a data processor and either: a) has earned or received \$10M or more of annual revenue through 300 or more transactions, or b) processes or maintains the personal information of 10,000 or more unique individuals during a calendar year.
 - Exempts various entities and information types, including information captured from patient by health entity or biometric information for certain approved uses, including for operations under HIPAA; personal information shared by individuals in the workplace or similar setting; and employee or entity-based member contact information.
 - Creates individual rights for consumers, including the right to have access to and portability of their personal information; the right to correct inaccurate personal information; the right to delete personal information; the right to know what personal information will be collected and processed before giving consent; the right to be provided with privacy policies; and the right to know names of third parties to which covered entities will disclose personal information and to refuse consent for such disclosure.

- Creates duties of confidentiality, care, and loyalty to consumers.
- Requires consent before personal information is collected and processed.
- Creates the Massachusetts Information Privacy Commission, which can impose civil penalties on covered entities.
- Creates a private right of action. Violations are also enforceable by the Massachusetts AG's office.
- Creates additional requirements for processing sensitive personal information, namely notice.
- No civil penalty should be (a) less than 0.15% of the annual global revenue of the entity or \$15,000, whichever is greater, per individual violation; or (b) more than 4% of the entity's global revenue or \$20M whichever is greater, if the commission assesses a civil administrative penalty for multiple violations that affect multiple individuals.
- Section 2 would go into effect immediately; remaining sections would go into effect 12 months after the Act.

Ohio

1. *Bill Title:* [Ohio Personal Privacy Act, H.B. No. 376](#)
2. *Current Status:* As of January 23, 2022, the bill had been introduced in the Ohio House and referred to the Government Oversight Committee.
3. *Key Provisions:*
 - Applies to businesses that conduct business in the state or produce products or services targeted to consumers in the state that either: a) have annual gross revenues generated in the state that exceed \$25M, b) control or process personal data of 100,000 or more consumers during a calendar year, or c) during a calendar year, derive over fifty percent of gross revenues from sale of personal data and process or control personal data of 25,000 or more consumers.
 - Exempts various entities and information types, including boards, commissions, agencies, and other entities of the state or of political subdivisions of the state; covered entities or business associates governed by HIPAA; financial institutions or data governed by GLBA; information governed by the Fair Credit Reporting Act and FERPA; and B2B transactions.
 - Creates individual rights for consumers, including the right to know their personal data is being collected and processed; the right to request access to and disclosure of personal data; the right to request deletion of their personal data; and the right to request that their personal information not be sold to third parties.
 - Creates affirmative defense if a business creates, maintains, and complies with a written privacy program that conforms to the National Institute of Standards and Technology (NIST) privacy framework.
 - Does not create a private right of action. Violations are only enforceable by the Ohio AG's office.
 - AG can seek civil penalties of up to \$5,000 for each violation.

- Creates a thirty-day cure period after the AG provides written notice. If entity cures violation and provides AG express written statement, no action will be initiated.

Washington, DC

1. *Bill Title:* [Uniform Personal Data Protection Act of 2021, Bill 24-451](#)
2. *Current Status:* As of January 23, 2022, the bill had been introduced in the Office of the Secretary and referred to the Committee on Judiciary and Public Safety.
3. *Key Provisions:*
 - Applies to controllers or processors that conduct business in D.C. or provide products or services directed to D.C. residents and either: a) maintain personal data of more than 50,000 District residents, b) earn more than fifty percent of their annual income from maintaining this data, or c) maintain data for incompatible or prohibited data practices.
 - Exempts various entities and activities, including processing governed by HIPAA, GLBA, FERPA, and COPPA; and agencies or instrumentalities of the District.
 - Creates individual rights for consumers, including the right to a copy of their data, and the right to have the collecting controller correct or amend data. There is no right to deletion of data.
 - Delineates prohibited data practices.
 - Requires that notice of the use of “incompatible data practices” be provided, as well as a reasonable opportunity to withhold consent to the practice.
 - Creates additional requirements for processing sensitive data when combined with an “incompatible data practice,” namely written consent.
 - Does not create a private right of action. Violations are enforceable by the D.C. AG’s office, and the AG can adopt rules to implement the law.
 - Adopts the same penalties as the D.C. Consumer Protection Procedures Act (CCPA), where the AG can recover civil penalty of up to \$5,000 for each violation (for first time violations), up to \$10,000 for each subsequent violation, economic damages, and the costs of the action and reasonable attorneys’ fees.
 - Would go into effect after approval by the Mayor.

Indiana (Senate bill)

1. *Bill Title:* [Senate Bill No. 358](#)
2. *Current Status:* As of January 23, 2022, the bill had been introduced in the Senate and referred to the Committee on Commerce and Technology.
3. *Key Provisions:*
 - Applies to businesses that collect consumers’ personal information, determine the purposes and means of the processing of the information (alone or jointly), do business in Indiana, and either: a) have annual gross revenues in excess of \$25M; b) buy, receive, sell, or share for commercial purposes the personal information of at least 50,000 consumers, households, or devices; or c) derive fifty percent or

more of annual revenues from selling information.

- Covered businesses must inform consumers of the categories of personal information collected; purposes for which the information is collected or used; whether the information will be sold or shared; the categories of personal sensitive information collected; and whether sensitive information is collected, sold, and shared and for what use.
- Creates individual rights for consumers, including the right to request personal information collected; the right to have personal information be deleted; the right to correct inaccurate personal information; the right to know what personal information is sold or shared; and the right to opt out of having their personal information be sold or shared.
- Incorporates privacy by design principles, such as requiring that businesses not collect sensitive personal information for additional purposes that are incompatible with the disclosed purposes, and not retain consumer's personal or sensitive information longer than is reasonably necessary. The bill also requires that businesses implement reasonable security procedures.
- Creates additional requirements for processing sensitive personal information.
- Does not create a private right of action. Violations are enforceable by the Indiana AG's office as a deceptive act. The AG can adopt rules to implement this bill.
- Would go into effect on July 1, 2022.

Indiana (House bill)

1. *Bill Title:* [House Bill 1261](#)
2. *Current Status:* As of January 23, 2022, the bill had been introduced in the House and referred to the Committee on Commerce, Small Business and Economic Development.
3. *Key Provisions:*
 - Applies to businesses that conduct business in Indiana, produce products or services that are marketed to Indiana residents, and control or process personal data of either: a) at least 100,000 consumers during a calendar year; or b) at least 25,000 consumers during a calendar year and derive more than fifty percent of gross revenue from the sale of personal data.
 - Exempts various entities and information types, including state government branches and political subdivisions; certain government entities; health care providers or covered entities governed by federal privacy law; and information governed by GLBA, and the Fair Credit Reporting Act.
 - Covered businesses must inform consumers, upon request, of the categories of personal information collected; the consumer's right to request specific pieces of information collected; certain categories of sources; the purposes for which the information is collected, sold, or shared; and the categories of third parties to whom information will be disclosed. They must also inform consumers of their right to request deletion of personal information.
 - Creates individual rights for consumers, including the right to opt out of having their

personal information sold or shared; and the right to restrict how businesses use their information.

- Consumers can limit business's use of the consumer's sensitive personal information.
- Does not create a private right of action. Violations are enforceable by the Indiana Division of Consumer Protection.
- Would go into effect on July 1, 2022.

Washington

1. *Bill Title:* [Washington Privacy Act, 2SSB 5062](#)
2. *Current Status:* In 2021, the bill was introduced in the Senate and the House, referred to multiple committees, and was substituted twice. In 2022, and as of January 24, the bill has been reintroduced in the Senate.
3. *Key Provisions:*
 - Applies to entities that conduct business in Washington or produce products or services that are targeted to Washington residents, and that satisfy one or more of the following: a) during a calendar year, control or process personal data of 100,000 consumers or more; or b) derive over 25 percent of gross revenue from the sale of personal data and process or control personal data of 25,000 consumers or more.
 - Exempts various entities and information types, including state and local government entities; covered entities or business associates governed by HIPAA and personal information covered by HIPAA; personal information collected, maintained, used, or disclosed pursuant to GLBA and the Fair Credit Reporting Act; and personal data governed by FERPA.
 - Creates individual rights for consumers, including the right to confirm whether personal data is being processed and to access these categories of data; the right to correct inaccurate personal data; the right to delete personal data; the right to obtain personal data in a portable and readily usable format; the right to opt out of the processing of personal data for targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer.
 - Incorporates privacy by design principles, such as data minimization, reasonable security practices, and purpose specification.
 - Requires data protection assessments.
 - Creates additional requirements for processing sensitive data.
 - Does not create a private right of action. Violations are only enforceable by the Washington AG's office.
 - Creates a thirty-day cure period after the AG provides a warning letter. If entity does not cure violation, the AG may bring an action.
 - Imposes civil penalties of up to \$7,500 for each violation. The AG can also recover costs of investigation, including reasonable attorneys' fees.
 - Would go into effect on July 31, 2022.

Mississippi

1. *Bill Title:* [Mississippi Consumer Data Privacy Act, SB 2330](#)
2. *Current Status:* As of January 24, 2022, the bill had been introduced in the Senate and referred to the Judiciary, Division A Committee.
3. *Key Provisions:*
 - Applies to businesses that control consumers' personal information, that determine the purposes and means of the processing of this information, that do business in Mississippi, and that satisfy one or more of the following: a) annual gross revenues in excess of \$10M; b) alone or in combination, annually buy, receive, sell or share for commercial purposes the information of 50,000 or more consumers, households, or devices; or c) derive fifty percent or more of annual revenues from selling this information.
 - Creates individual rights for consumers, including the right to know what personal information is being collected about them; the right to know their information is sold or disclosed and to whom; the right to decline or opt-out of the sale of their personal information; the right to access their personal information that has been collected; and the right to receive equal service and price, even if they exercise their rights.
 - Creates a private right of action. Violations are also enforceable by the Mississippi AG's office.
 - Imposes civil penalties of up to \$7,500 for each violation. Consumers can recover damages between \$100 and \$750 per consumer and per incident, or actual damages, whichever is greater.
 - Creates a thirty-day cure period, excluding for actions for actual pecuniary damages suffered.
 - Would go into effect on July 1, 2023.

Kentucky

1. *Bill Title:* [SB 15](#)
2. *Current Status:* As of January 24, 2022, the bill had been introduced in the Senate and referred to the Economic Development, Tourism, & Labor Committee.
3. *Key Provisions:*
 - Applies to persons that conduct business in Kentucky or produce products or services that are targeted to Kentucky residents and that during a calendar year: a) control or process personal data of at least 10,000 consumers; or b) derive over forty percent of gross revenue from the sale of personal data.
 - Exempts various entities and information types, including state and local agencies; financial institutions subject to the GLBA; covered entities or business associates governed by HIPAA; and information governed by the Fair Credit Reporting Act and FERPA.
 - Creates individual rights for consumers, including the right to confirm whether their

data is being processed; the right to access their data; the right to delete data provided by them; the right to obtain a copy of the personal data they previously provided to the controller in a portable and readily usable format; the right to opt out of targeted advertising; the right to opt out of tracking; and the right to opt out of the sale or sharing of personal data.

- Incorporates privacy by design principles, such as purpose limitation.
- Requires controllers to conduct a data protection impact assessment.
- Creates additional requirements for processing sensitive data.
- Does not create a private right of action. Violations are only enforceable by the Kentucky AG's office.
- Imposes civil penalties of up to \$7,500 for each violation. The AG may recover reasonable expenses incurred in investigating and preparing the case, including attorneys' fees.
- Creates a thirty-day cure period after the AG provides written notice. If entity cures violation and provides AG express written statement, no action for statutory damages will be initiated.
- Would go into effect on January 1, 2024.

Nebraska

1. *Bill Title:* [LB 1188, Adoption of the Uniform Personal Data Protection Act](#)
2. *Current Status:* As of January 24, 2022, the bill had been referred to the Banking, Commerce, and Insurance Committee.
3. *Key Provisions:*
 - Applies to controllers or processors that conduct business in Nebraska or provide products or services directed to Nebraska residents and either: a) maintain personal data of more than 50,000 Nebraska residents during a calendar year, b) earn more than fifty percent of their annual income from maintaining this data during a calendar year, or c) maintain data for incompatible or prohibited data practices.
 - Exempts various activities, including processing governed by HIPAA, GLBA, FERPA, COPPA, and the Fair Credit Reporting Act.
 - Creates individual rights for consumers, including the right to a copy of their data, and the right to have the collecting controller correct or amend data. There is no right to deletion of data.
 - Creates additional requirements for processing sensitive data.
 - Delineates prohibited data practices.
 - Requires that notice of the use of "incompatible data practices" be provided, as well as a reasonable opportunity to withhold consent to the practice. Requires express consent for the processing of "sensitive data" using an "incompatible data practice."
 - Does not create a private right of action. Violations are enforceable by the Nebraska AG, and the AG can adopt rules to implement the law.
 - Violations of the law would be enforceable as violations of Nebraska's Consumer

Protection Act.

- Would go into effect on January 1, 2023.

Pennsylvania

1. *Bill Title:* [Consumer Data Protection Act, H.B. 2557](#)
2. *Current Status:* As of January 25, 2022, the bill had been introduced in the Senate and referred to the Consumer Affairs Committee.
3. *Key Provisions:*
 - Applies to persons that conduct business in Pennsylvania or produce goods, products or services that are sold or offered for sale to Pennsylvania residents and that: a) during a calendar year, control or process personal data of at least 100,000 consumers; or b) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.
 - Exempts various entities and information types, including the State and political subdivisions of the State and related agencies and offices; financial institution or data subject to the GLBA; covered entity or business associate, or health information governed by HIPAA; personal data regulated by FERPA; and the use of personal information associated with activities regulated by the FCRA.
 - Creates individual rights for consumers, including the right to confirm whether the controller is processing the consumer's personal data and to access the personal data; the right to correct inaccuracies in the consumer's personal data; the right to delete personal data provided by the consumer or obtained by the controller about the consumer; the right to obtain a copy of the data in a portable and readily usable format; and the right to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.
 - Incorporates privacy by design principles, such as purpose limitation and reasonable security practices.
 - Creates additional requirements for processing sensitive data, namely written consent.
 - Requires controllers to conduct and document a data protection assessment for certain processing activities involving personal data.
 - Does not create a private right of action. Violations are enforceable by the Pennsylvania AG, and the AG can adopt regulations to implement the law.
 - The AG may seek civil penalties of up to \$7,500 for each violation.
 - Creates a 30-day cure period after the AG provides written notice. If entity cures violation and provides AG express written statement, no action will be initiated.
 - Would go into effect on January 1, 2023, or in 18 months, whichever is later.

Authors



Kirk J. Nahra

PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



Ali A. Jessani

COUNSEL

✉ ali.jessani@wilmerhale.com

☎ +1 202 663 6105