

State Privacy Law Updates—Privacy Patchwork Additions

By Sanford P. Shatz and Paul J. Lysobey*

INTRODUCTION¹

Since the last publication of this survey, state legislatures have continued the trend of enacting comprehensive privacy laws.² In this span, the following comprehensive data privacy laws were enacted: the Delaware Personal Data Privacy Act (“Delaware PDPA”),³ the New Jersey Act Concerning Online Services, Consumers, and Personal Data (“New Jersey Privacy Act”),⁴ the New Hampshire Act Relative to the Expectation of Privacy (“New Hampshire Privacy Act”),⁵ the Kentucky Consumer Data Protection Act (“Kentucky CDPA”),⁶ the Nebraska Data Privacy Act (“Nebraska DPA”),⁷ the Maryland Online Data Privacy Act of 2024 (“Maryland ODPa”),⁸ the Minnesota Consumer Data Privacy Act (“Minnesota CDPA”),⁹ and the Rhode Island Data Transparency and Privacy Protection Act (“Rhode Island DTPPA”).¹⁰

* Sanford P. Shatz is a Partner at Wright, Finlay & Zak, LLP in Newport Beach, California. Paul J. Lysobey (CIPP/US) is an Associate at Wegman Hessler in Cleveland, Ohio.

1. This survey is one in a series of works covering recent updates in various areas of consumer financial services law. For an overview of the other surveys in this issue of *The Business Lawyer*, see John L. Ropiequet, Eric J. Mogilnicki, Sabrina A. Neff & Christopher K. Odinet, *Introduction to the 2025 Annual Survey of Consumer Financial Services Law*, 80 BUS. LAW. 531 (2025) (in this *Annual Survey*).

2. This survey is a continuation of surveys previously published regarding privacy laws as part of the *Annual Survey of Consumer Financial Services Law*. See Sanford P. Shatz & Paul J. Lysobey, *State Privacy Law Updates—An Ever-Growing List of States*, 79 BUS. LAW. 539 (2024) (in the 2024 *Annual Survey*) [hereinafter *Ever-Growing List*]; Sanford P. Shatz & Paul J. Lysobey, *Privacy Laws Continue Their Spread Across the Country*, 78 BUS. LAW. 551 (2023) (in the 2023 *Annual Survey*); Sanford P. Shatz & Paul J. Lysobey, *Update on the California Consumer Privacy Act and Other States’ Actions*, 77 BUS. LAW. 539 (2022) (in the 2022 *Annual Survey*); Sanford P. Shatz & Paul J. Lysobey, *The California Consumer Privacy Act of 2018 Updated: More Protection in the Quest to Access and Protect Personal Information*, 77 BUS. LAW. 539 (2021) (in the 2021 *Annual Survey*). This survey provides an update on state privacy laws enacted through June 2024 that were not covered in the prior surveys.

3. See DEL. CODE ANN. tit. 6, §§ 12D-101–12D-111 (enacted Sept. 11, 2023, effective Jan. 1, 2025).

4. See N.J. REV. STAT. §§ 56:8-166.4–56:8-166.19 (enacted Jan. 16, 2024, effective Jan. 15, 2025).

5. See N.H. REV. STAT. §§ 507-H:1–507-H:12 (enacted Mar. 6, 2024, effective Jan. 1, 2025).

6. H.R. 15, 2024 Leg., Reg. Sess. (Ky. 2024) (enacted Apr. 4, 2024, effective Jan. 1, 2026).

7. L.B. 1074, 108th Leg., 2d Reg. Sess. (Neb. 2024) (enacted Apr. 17, 2024, effective Jan. 1, 2025).

8. See MD. CODE ANN., COM. LAW §§ 14-4601–14-4614 (enacted May 9, 2024, effective Oct. 1, 2025).

9. See MINN. STAT. §§ 3250.01–3250.11 (enacted May 24, 2024, effective July 31, 2025).

10. See R.I. GEN. LAWS §§ 6-48.1-1–6-48.1-10 (enacted June 29, 2024, effective Jan. 1, 2026).

These state laws have followed comprehensive data privacy legislation enacted in prior years in California, Colorado, Connecticut, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia.¹¹ This survey provides an overview of the newly enacted state privacy laws through June 2024. At a high level, the newly enacted laws in Delaware, New Jersey, New Hampshire, Kentucky, Nebraska, Maryland, Minnesota, and Rhode Island generally adopt the major substantive provisions and themes from earlier privacy laws, with each law specifying to whom it applies, exemptions from applicability, consumer rights, responsibilities of controllers, and how the laws are enforced. This survey addresses these major themes and notes major differences between the eight new state laws. However, it does not address every aspect of each law and is meant only to provide a general overview of the common concepts in each law. This survey also provides an update on laws enacted in prior years that are currently in effect, or that will be in effect soon.

EIGHT NEW STATE PRIVACY LAWS

Like current state privacy laws, the privacy laws in Delaware, New Jersey, New Hampshire, Kentucky, Nebraska, Maryland, Minnesota, and Rhode Island apply to persons engaging in activities related to controlling and processing of personal data of consumers, provided that the entity in question meets certain threshold requirements that trigger the applicability of the respective law. Each of these laws has a slightly different scope and applicability, and, as a result, it is important to first understand each law and to whom it applies.

APPLICABILITY

The Delaware PDPA, the Maryland ODPa, and the Rhode Island DTPPA have substantially similar applicability and scope provisions. Using the Delaware PDPA as a baseline, the law applies to:

[P]ersons that conduct business in [Delaware] or persons that produce products or services that are targeted to residents of [Delaware] and that during the preceding calendar year did any of the following:

- (1) Controlled or processed the personal data of not less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.
- (2) Controlled or processed the personal data of not less than 10,000 consumers and derived more than 20 percent of their gross revenue from the sale of personal data.¹²

Maryland and Rhode Island have almost identical applicability requirements.¹³ In addition, the New Hampshire law's applicability provision is similar, the only difference being that the New Hampshire Privacy Act uses a 25 percent

11. See *Ever-Growing List*, *supra* note 1.

12. See DEL. CODE ANN. tit. 6, § 12D-103(a).

13. See MD. CODE ANN., COM. LAW § 14-4602(1)–(2); R.I. GEN. LAWS § 6-48.1-4(a) (note that the scope of the Rhode Island DTPPA is limited specifically to “for-profit entities”).

gross revenue threshold instead of the 20 percent threshold used in Maryland and Rhode Island.¹⁴

The scope of the laws in New Jersey, Kentucky, and Minnesota is also similar enough to group them together. As a point of reference, the New Jersey Privacy Act applies to:

[C]ontrollers that conduct business in [New Jersey] or produce products or services that are targeted to residents of [New Jersey], and that during a calendar year either:

- (a) control or process the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction; or
- (b) control or process the personal data of at least 25,000 consumers and the controller derives revenue, or receives a discount on the price of any goods or services, from the sale of personal data.¹⁵

The Kentucky CDPA applies to:

[P]ersons that conduct business in [Kentucky] or produce products or services that are targeted to residents of the Commonwealth and that during a calendar year control or process personal data of at least:

- (a) One hundred thousand (100,000) consumers; or
- (b) Twenty-five thousand (25,000) consumers and derive over fifty percent (50%) of gross revenue from the sale of personal data.¹⁶

The Minnesota CDPA applies to:

[L]egal 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:

- (1) during a calendar year, controls or processes personal data of 100,000 consumers or more, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- (2) derives over 25 percent of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.¹⁷

One common characteristic between the privacy laws in New Jersey, Kentucky, and Minnesota is that the laws in each of these states provide that the respective state law will apply if a business conducts business in the state and controls or processes the data of at least 100,000 consumers in a calendar year.¹⁸ However, while the New Jersey and Minnesota laws exclude from the 100,000-consumer calculation any data processed “solely for the purpose of

14. See N.H. REV. STAT. § 507-H:2(a)–(b).

15. See N.J. REV. STAT. § 56:8-166.5.

16. Ky. H.B. 15, § 2(1)(a)–(b).

17. See MINN. STAT. § 3240.03(a).

18. See N.J. REV. STAT. § 56:8-166.5; Ky. H.B. 15, § 2(1)(a)–(b); MINN. STAT. § 3250.03(a).

completing a payment transaction,” the Kentucky law does not include such a limitation.¹⁹ These laws each also provide a second applicability prong that will trigger the privacy law if a business controls or processes the data of 25,000 or more consumers and derives a certain percentage of gross revenue from the sale of personal data (any amount of gross revenue in New Jersey, 50 percent gross revenue in Kentucky, 25 percent gross revenue in Minnesota).²⁰ Therefore, although these three state laws are similar, they differ significantly on the gross revenue threshold related to the sale of personal data that is needed to trigger the law under the second prong.

Lastly, the Nebraska DPA’s applicability section is in its own category, as it provides the broadest reach and essentially applies to any entity that conducts business in Nebraska and processes or engages in the sale of personal data.²¹ This means that an entity could be subject to the Nebraska DPA if it sells any amount of personal data for any number of consumers.

As with most other state privacy laws, the entity subject to each of these laws is designated as a “controller” or “processor” of personal data. A “controller” is generally defined to mean a person who “alone or jointly with others, determines the purpose and means of processing personal data.”²² “Processor” is defined to mean a person “that processes personal data on behalf of a controller” and most states laws define “processing” to mean “any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.”²³ Each of these laws also generally provides a similar definition for “personal data,” and defines the term to essentially mean information that is “linked to or reasonably linkable to an identified individual.”²⁴ However, the state privacy laws generally define “personal data” to exclude “de-identified data” and “publicly available information.”²⁵

19. See N.J. REV. STAT. § 56:8-166.5; Ky. H.B. 15, § 2(1)(a)–(b); MINN. STAT. § 3250.03(a).

20. See N.J. REV. STAT. § 56:8-166.5; Ky. H.B. 15, § 2(1)(a)–(b); MINN. STAT. § 3250.03(a).

21. Neb. L.B. 1074, § 3. Note that the Nebraska DPA’s applicability section also states that the law will apply only if a person “[i]s not a small business as determined under the federal Small Business Act, . . . , except to the extent that section 18 of [the Nebraska DPA] applies” to such a person. Neb. L.B. 1074, § 3. Section 18 prohibits the sale of “sensitive data” unless the consumer provides prior consent to the sale. Neb. L.B. 1074, § 18.

22. See DEL. CODE ANN. tit. 6, § 12D-102; N.J. REV. STAT. § 56:8-166.4; N.H. REV. STAT. § 507-H:1; Ky. H.B. 15, § 1; Neb. L.B. 1074, § 2; MD. CODE ANN., COM. LAW § 14-4601; MINN. STAT. § 3250.02; R.I. GEN. LAWS § 6-48.1-2.

23. See DEL. CODE ANN. tit. 6, § 12D-102. See also N.J. REV. STAT. § 56:8-166.4; N.H. REV. STAT. § 507-H:1; Ky. H.B. 15, § 1; Neb. L.B. 1074, § 2; MD. CODE ANN., COM. LAW § 14-4601; MINN. STAT. § 3250.02; R.I. GEN. LAWS § 6-48.1-2. The New Jersey Privacy Act specifies that “processing . . . also includes the actions of a controller directing a processor to process personal data.” See N.J. REV. STAT. § 56:8-166.5.

24. See DEL. CODE ANN. tit. 6, § 12D-102. See also N.J. REV. STAT. § 56:8-166.4; N.H. REV. STAT. § 507-H:1; Ky. H.B. 15, § 1; Neb. L.B. 1074, § 2; MD. CODE ANN., COM. LAW § 14-4601; MINN. STAT. § 3250.02; R.I. GEN. LAWS § 6-48.1-4(7).

25. See DEL. CODE ANN. tit. 6, § 12D-102; N.J. REV. STAT. § 56:8-166.4; N.H. REV. STAT. § 507-H:1; Ky. H.B. 15, § 1; Neb. L.B. 1074, § 2; MD. CODE ANN., COM. LAW § 14-4601; MINN. STAT. § 3250.02; R.I. GEN. LAWS § 6-48.1-2.

EXEMPTIONS

Each of the privacy laws addressed in this survey includes a comprehensive list of persons and types of data that are not subject to the respective law. Notably for financial institutions, most of these state laws provide some form of an exemption for financial institutions governed by or data subject to the Gramm-Leach-Bliley Act (“GLBA”).²⁶ The New Jersey Privacy Act, the Kentucky CDPA, the Nebraska DPA, the Maryland ODPa, and the Rhode Island DTPPA exempt financial institutions, affiliates of financial institutions, and data that is subject to the GLBA.²⁷ Similarly, the New Hampshire Privacy Act exempts “a financial institution or data subject to” the GLBA, but does not expressly exempt affiliates of financial institutions.²⁸ The Delaware PDPA exempts “financial institutions or affiliates subject to” the GLBA, but does not specifically provide an exemption for data subject to the GLBA.²⁹

In contrast, the Minnesota law has deviated from most other state privacy laws enacted to date by not including a clear exemption for financial institutions subject to the GLBA.³⁰ While the Minnesota CDPA provides a data-level exemption for personal data collected, processed, sold, or disclosed pursuant to the GLBA, the law does not include a typical entity-level exemption for financial institutions. The Minnesota CDPA does not apply to (among other things):

[I]nformation that is: . . . (iv) originated from, or intermingled with, information described in clause (9) [GLBA data-level exemption] and that a licensed residential mortgage originator, as defined under section 58.02, subdivision 19, or residential mortgage servicer, as defined under section 58.02, subdivision 20, collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified in clause (9); or (v) originated from, or intermingled with, information described in clause (9) [GLBA data-level exemption] and that a nonbank financial institution, as defined by section 46A.01, subdivision 12, collects, processes, uses, or maintains in the same manner as required under the laws and regulations specified in clause (9);

. . . .

(9) personal data collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law.³¹

Therefore, while the Minnesota CDPA does not include an entity-level exemption for GLBA financial institutions, the Minnesota CDPA exempts certain other data used by a licensed residential mortgage originator, residential mortgage servicer,

26. Pub. L. No. 106-102, tit. V, § 501, 113 Stat. 1346 (1999) (codified as amended at 15 U.S.C. §§ 6801–6809 (2024)).

27. See N.J. REV. STAT. § 56:8-166.13(b); Ky. H.B. 15, § 2; Neb. L.B. 1074, § 3(2); MD. CODE ANN., COM. LAW § 14-4603(a)(3); R.I. GEN. LAWS § 6-48.1-3.

28. See N.H. REV. STAT. § 507-H:2(I)(e).

29. See DEL. CODE ANN. tit. 6, § 12D-103(b)(2).

30. See MINN. STAT. § 3250.03(Subd. 2)(a)(6)(iv)–(v), (a)(9).

31. See MINN. STAT. § 3250.03(Subd. 2)(a)(6)(iv)–(v), (a)(9).

or a “nonbank financial institution”³² if such data is “originated from, or intermingled with,” exempt GLBA data.³³ It is unclear how this “intermingled” data exemption will operate in practice. However, financial institutions subject to GLBA that would typically rely on the entity-level exemption often found in other state privacy laws should be aware that the Minnesota CDPA does not provide such a blanket exemption for financial entities.

Among many other exemptions listed in these statutes, notable exemptions common among many of these laws include: governmental entities; protected health information under the Health Insurance Portability and Accountability Act;³⁴ certain types of data subject to regulation under the Fair Credit Reporting Act;³⁵ and data processed or maintained in the context of employment purposes for purposes such as maintaining emergency contact information or to administer benefits.³⁶

CONSUMER PERSONAL DATA RIGHTS

At a broad level, these privacy laws establish the following rights for consumers: the right to confirm whether a controller is processing the consumer’s personal data and the right to access the consumer’s personal data; the right to correct inaccuracies in a consumer’s personal data that the consumer provided to the controller; the right to delete the consumer’s personal data; the right to obtain a copy of the consumer’s personal data; and the right to opt out of the processing of the consumer’s personal data for certain purposes, including targeted advertising or the sale of personal data.³⁷

EXERCISING CONSUMER RIGHTS AND RESPONDING TO REQUESTS

A consumer may exercise a right by submitting a request to a controller specifying the rights the consumer intends to exercise.³⁸ The process for responding to a consumer request is similar among the laws in each of these states. As a general rule, the controller must respond to a consumer request no later than

32. The definition for a “nonbank financial institution” is a cross reference to a definition for “financial institution” under another Minnesota law, which defines the term to mean “a consumer small loan lender . . . , a person owning or maintaining electronic financial terminals . . . , a trust company . . . , a loan and thrift company . . . , a currency exchange . . . , a money transmitter . . . , a sales finance company . . . , a regulated loan lender . . . , a residential mortgage originator or servicer . . . , a student loan servicer . . . , a credit service organization . . . , a debt management service provider or person providing debt management services . . . , or a debt settlement service provider or person providing debt settlement services.” MINN. STAT. § 46A.01(Subd. 12).

33. MINN. STAT. § 3250.03(Subd. 2)(a)(6)(iv)–(v),

34. See, e.g., DEL. CODE ANN. tit. 6, § 12D-103.

35. *Id.*

36. *Id.*

37. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.10; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 7; MD. CODE ANN., COM. LAW § 14-4605; MINN. STAT. § 3250.05; R.I. GEN. LAWS § 6-48.1-5.

38. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.10; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 7; MD. CODE ANN., COM. LAW § 14-4605; MINN. STAT. § 3250.05; R.I. GEN. LAWS § 6-48.1-5.

forty-five days after receipt of the consumer's request.³⁹ The controller may extend this period for an additional forty-five days if reasonably necessary due to the amount or complexity of requests.⁴⁰ If the controller has grounds to extend the initial forty-five-day period, the controller must inform the consumer before the initial forty-five-day period expires of the length of the extension and the reasons for the extension.⁴¹ If a controller declines to act in response to a request, the controller must inform the consumer of the reasons for not taking action no later than forty-five days after receipt of the request.⁴²

If the controller fails to act under the respective state privacy laws, in addition to informing the consumer of the reasons for not taking action, the controller must inform the consumer in writing with information regarding how to appeal the decision.⁴³ The appeal is generally done through an internal process that the controller is required to establish.⁴⁴ If an appeal is denied the controller also must provide the consumer information regarding how to contact the respective state attorney general to submit a complaint.⁴⁵

DUTIES OF CONTROLLERS

Each of the newly enacted laws generally provides similar duties for controllers. Among other duties specified under each law, common duties include, among others: limiting collection of data to what is "adequate," "relevant," and "necessary" with respect to the processing purposes as disclosed to the consumer; implementing security practices and safeguards to protect the "confidentiality, integrity, and accessibility" of personal data; not processing personal data in violation of state or federal laws prohibiting discrimination, unless a statutory exception applies; not discriminating against consumers for exercising their consumer rights; the duty not to process "sensitive data" about a consumer without obtaining the consumer's consent, with additional requirements applying for

39. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

40. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

41. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

42. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

43. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

44. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

45. See DEL. CODE ANN. tit. 6, § 12D-104; N.J. REV. STAT. § 56:8-166.7; N.H. REV. STAT. § 507-H:4; Ky. H.B. 15, § 3; Neb. L.B. 1074, § 9; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.05 (Subd. 5); R.I. GEN. LAWS § 6-48.1-6.

processing sensitive data regarding a known child; and providing an effective mechanism for a consumer to revoke consent.⁴⁶ Controllers also must generally provide consumers with a “reasonably accessible, clear, and meaningful” privacy notice that includes certain required content.⁴⁷

ENFORCEMENT AUTHORITY

Under all of the privacy laws addressed in this survey, the attorney general in each respective state has exclusive authority to enforce the law and none of these laws contains a private right of action.⁴⁸ Some of these laws also provide either an optional or mandatory right-to-cure period before the attorney general can bring an enforcement action. The New Jersey Privacy Act, the New Hampshire Privacy Act, the Kentucky CDPA, the Nebraska DPA, and the Minnesota CDPA require the respective attorney general to provide a cure period (thirty days in New Jersey, Kentucky, Nebraska, and Minnesota, sixty days in New Hampshire) before bringing an enforcement action.⁴⁹ However, the New Jersey Privacy Act’s cure provision will expire eighteen months following the effective date of the law, the New Hampshire Privacy Act’s cure provision will expire on December 31, 2025, and the Minnesota CDPA’s cure provision will expire on January 31, 2026.⁵⁰ In contrast, the Delaware PDPA and the Maryland ODPa provide that the enforcement authority may issue a notice of the violation and provide a sixty-day cure period, but there is no mandatory cure period under these laws.⁵¹ The Rhode Island DTPPA does not provide for a statutory right-to-cure period.

Some of the state privacy laws also provide for a specific civil penalty of up to a certain amount for each violation. For example, the Kentucky CDPA, the Nebraska Privacy Act, and the Minnesota CDPA allow for the attorney general to recover a civil penalty of up to \$7,500 per violation.⁵²

UPDATE ON CURRENTLY ENACTED LAWS

The data privacy laws addressed in this survey have joined existing comprehensive privacy laws enacted in prior years in California, Colorado, Connecticut,

46. See DEL. CODE ANN. tit. 6, § 12D-10. See also N.J. REV. STAT. §§ 56:8-166.12; 56:8-166.8; N.H. REV. STAT. § 507-H:6; Ky. H.B. 15, § 4; Neb. L.B. 1074, § 12; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.07(Subd. 2)–(Subd. 3); R.I. GEN. LAWS §§ 6-48.1-4; 6-48.1-7. The exact terminology may differ between the laws of each state.

47. See DEL. CODE ANN. tit. 6, § 12D-10. See also N.J. REV. STAT. § 56:8-166.6; N.H. REV. STAT. § 507-H:6; Ky. H.B. 15, § 4; Neb. L.B. 1074, § 12; MD. CODE ANN., COM. LAW § 14-605; MINN. STAT. § 3250.10(d); R.I. GEN. LAWS §§ 6-48.1-4; 6-48.1-7. The exact terminology may differ between the laws of each state.

48. See DEL. CODE ANN. tit. 6, § 12D-111 (the Delaware Department of Justice has enforcement authority); N.J. REV. STAT. § 56:8-166.19; N.H. REV. STAT. § 507-H:11; Ky. H.B. 15, § 9; Neb. L.B. 1074, § 19; MD. CODE ANN., COM. LAW § 14-4614; MINN. STAT. § 3250.10; R.I. GEN. LAWS § 6-48.1-8.

49. See N.J. REV. STAT. § 56:8-166.17; N.H. REV. STAT. § 507-H:11; Ky. H.B. 15, § 9; Neb. L.B. 1074, § 19; MINN. STAT. § 3250.10.

50. See N.J. REV. STAT. § 56:8-166.17; N.H. REV. STAT. § 507-H:11; MINN. STAT. § 3250.10.

51. See DEL. CODE ANN. tit. 6, § 12D-111; MD. CODE ANN., COM. LAW § 14-4614.

52. See Ky. H.B. 15, § 9; Neb. L.B. 1074, § 19; MINN. STAT. § 3250.10.

Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia.⁵³ Many of these laws are already in effect or will become effective soon. The effective dates of privacy laws enacted in prior years are:

- January 1, 2023: The California Consumer Privacy Act, as amended by the California Privacy Rights Act, and the Virginia Consumer Data Protection Act.⁵⁴
- July 1, 2023: The Colorado Privacy Act and the Connecticut Data Privacy and Online Monitoring Act.⁵⁵
- December 31, 2023: The Utah Consumer Privacy Act.⁵⁶
- July 1, 2024: Oregon Consumer Privacy Act.⁵⁷
- October 1, 2024: Montana Consumer Data Privacy Act.⁵⁸
- January 1, 2025: Iowa Consumer Data Protection Act and the Texas Data Privacy and Security Act.⁵⁹
- July 1, 2025: Tennessee Information Protection Act.⁶⁰
- January 1, 2026: Indiana Consumer Data Protection Act.⁶¹

As a result, entities subject to these laws should take note of the impending effective dates and be aware of which laws are already in effect. Entities should also be cognizant of the scope, applicability, and new compliance requirements imposed by each law.

53. See *Ever-Growing List*, *supra* note 1.

54. CAL. CIV. CODE §§ 1798.100–1798.199.100; VA. CODE ANN. §§ 59.1-575–59.1-584.

55. COLO. REV. STAT. §§ 6-1-1301–6-1-1313; CONN. GEN. STAT. § 42-515–42-525.

56. UTAH CODE ANN. §§ 13-61-101–13-61-404.

57. OR. REV. STAT. §§ 646A.570–646A.589.

58. MONT. CODE ANN. §§ 30-14-2801–30-14-2817.

59. IOWA CODE §§ 715D.1–715D.9; TEX. BUS. & COM. CODE ANN. §§ 541.001–541.205.

60. TENN. CODE ANN. §§ 47-18-3201–47-18-3214.

61. IND. CODE §§ 24-15-4-1–24-15-11-2.