NELSON LAW LLC
LAW OF MOTION

745 Fifth Avenue
Suite 500
New York, NY 10151-0099
nelson.legal

I. Federal Privacy Laws and Regulations

Unlike in the EU, where the General Data Protection Regulation (GDPR) sets a baseline, the United States does not have a broadly applicable federal law or regulation that governs the collection and use of personal information and data. Federal lawmakers have tried for years to enact uniform standards, including as recently as last year with the proposed American Data Privacy Protection Act ("ADPPA"), which, according to the International Association of Privacy Professionals ("IAPP"), is "the closest U.S. Congress has ever been to passing comprehensive federal privacy legislation" and has support of "some factions of the U.S. Federal Trade Commission." While ADPPA was referred favorably out of Committee, Congress did not act on it before the end of the term. Sources such as the National Press Foundation expect the bill's sponsors to reintroduce it this year.

If the ADPPA were to be enacted, it could have implications for the collection and use of Vehicle Performance Data ("VPD"). As drafted, ADPPA would provide heightened protection to "precise geolocation information that reveals the past or present actual physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals." Sec. 2(22)(A)(vi) (Sensitive Covered Data). ADPPA also would expressly restrict and prohibit all "covered entities"—*i.e.*, any entity or person that collects, processes, or transfers covered data and is subject to certain federal trade and communications acts—from transferring precise geolocation information to a third party "unless transferred to another device or service of such individual with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the precise geolocation information will be transferred with such a notice provided for each instance in which such transfer is to occur absent a search warrant or exigent circumstances." Sec. 102(a)(2).

While not a comprehensive data privacy law, the Federal Driver Privacy Act of 2015 arguably implicates VPD. That Act limits data retrieval from EDRs and expressly rests ownership of EDR data with the owner or lessee of the vehicle. Specifically, it provides that "[a]ny data retained by an event data recorder (defined in section 563.5 of title 49, Code of Federal Regulations), regardless of when the motor vehicle in which it is installed was manufactured, is the property of the owner, or in the case of a leased vehicle, the lessee of the motor vehicle in which the event data recorder is installed." Driver Privacy Act of 2015, sec. 24302(a) ("Limitations on Data Retrieval from Vehicle Event Data Recorders"). "Event Data Recorder" as defined in section 563.5 means "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event. For the purposes of this definition, the event data do not include audio and video data."

For more information on federal legislative efforts related to data privacy generally, the IAPP maintains a helpful "US Federal Privacy Legislation Tracker" on its website.

Outside of official lawmaking, according to its website page dedicated to "Vehicle Data Privacy," NHTSA works closely with the Federal Trade Commission "to facilitate the protection of consumer information" that may be collected though vehicle technologies:

> A recent highlight of this ongoing dialogue was NHTSA's sponsorship with the FTC of the June 2017 workshop examining consumer privacy and security issues posed by automated and connected motor vehicles. In November 2017, *ADS 2.0: A Vision for Safety* replaced the FAVP as the policy framework and NHTSA's operating guidance for ADS. NHTSA intended *A Vision for Safety* to be a clearer, more streamlined and less burdensome guidance document.

II. State Privacy Laws and Regulations

Without comprehensive federal guidance, legislative activity in the area of data privacy has been concentrated at the state level, with several states having enacted or now considering privacy laws similar to GDPR:

- The legislatures of California, Virginia, Colorado, Utah, and Connecticut each have passed state level privacy laws, all of which are or will be effective in 2023. Under implementing regulations, companies operating in these five states must disclose what they are doing with an individual consumer's data—broadly speaking, it is the consumer's right to access, delete, or move his/her data.

- Other state legislatures including those in Washington, Oregon, Oklahoma, Iowa, Minnesota, Indiana, Kentucky, Tennessee, New York, Vermont, and New Hampshire have proposed privacy laws in committee as of this writing. Several other states have recently introduced bills. In total, just under half of the states have enacted or are presently considering laws to govern the treatment of consumer data in their jurisdictions.

IAPP also provides a useful tracker for state legislative activity in this space.

With respect to vehicle data, the five state privacy laws presently enacted do not provide much explicit protection, although some provisions likely implicate the collection and storage of VPD. The following provides an overview:

California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), effective 2023.

- If a business collects personal information about a consumer, the business "shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether that personal information is sold, in a clear and conspicuous manner at the location." Cal. Civ. Code § 1798.100(b).

- Generally, a consumer has a right to opt-out of the sale or sharing of personal information about the consumer, and businesses that sell consumer personal information are required to provide notice and inform consumers of the right to opt out. Cal. Civ. Code § 1798.120. But, an exception to this general rule allows a vehicle dealer and the manufacturer to share vehicle/ownership information for the purpose of repair, provided the dealer and manufacturer warrant no other use. Cal. Civ. Code § 1798.145(g)(1).

- "Vehicle information" is expressly defined to mean "the vehicle information number, make, model, year, and odometer reading." Cal. Civ. Code § 1798.145(g)(3).

Virginia Consumer Data Protection Act of 2021, effective 2023.

- The Virginia Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined to mean any information that is linked or reasonably linkable to an identified or identifiable natural person." It does not include "de-identified data or publicly available information." Va. Code § 59.1-575. In addition, "sensitive data" is defined to include "precise geolocation data," and the Act restricts processing of such data without obtaining consumer consent. Va. Code §§ 59.1-575; 59.1-578(A)(5).

- The Act specifically exempts from its scope "personal data collected, processed, sold, or disclosed in compliance with the Federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.)." Va. Code § 59.1-576(C)(11). That Act regulates the sharing of DMV records other than for permitted uses, largely related to law enforcement and safety.

Colorado Privacy Act of 2021, effective 2023.

- The Colorado Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as "information that is linked or reasonably linkable to an identified or identifiable individual." It does not include "de-identified data or publicly available information." Colo. Rev. Stat. Ann. § 6-1-1303(17). "Identified or identifiable individual" is defined as an "individual who can be readily identified" including through reference to "specific geolocation data." Colo. Rev. Stat. Ann. § 6-1-1303(16).

- The Act specifically exempts from its scope "personal data . . . collected, processed, sold, or disclosed pursuant to the Federal Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq." Colo. Rev. Stat. Ann. § 6-1-1304(2)(j).

Utah Consumer Privacy Act of 2022, effective 2023.

- The Utah Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as "information that is linked or reasonably linkable to an identified or identifiable individual." It does not include "de-identified data, aggregated data, or publicly available information." Utah Code Ann. § 13-61-101(24). In addition, "sensitive data" is defined to include "precise geolocation data," and the Act restricts processing of such data without "clear notice and an opportunity to opt out of the processing." Utah Code Ann. § 13-61-302(3).

- The Act specifically exempts from its scope "personal data collected, processed, sold, or disclosed in accordance with the Federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.)." Utah Code Ann. § 13-61-102(2)(l).

- We note in addition that the Utah Motor Vehicle Event Data Recorder Act specifically provides that event data recorded on an event data recorder is private and is the personal information of the motor vehicle's owner.

Connecticut Act Concerning Personal Data Privacy and Online Monitoring of 2022, aka Connecticut Data Privacy Act, effective 2023.

- The Connecticut Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as "information that is linked or reasonably linkable to an identified or identifiable individual." It does not include "de-identified data or publicly available information." Conn. Pub. Act No. 22-15 § 1(18). In addition, "sensitive data" is defined to include "precise geolocation data," which is defined in turn to mean "information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet." Conn. Pub. Act No. 22-15 § 1(19), (27). "Sensitive data" may not be processed without consumer consent. Conn. Pub. Act No. 22-15 § 6(a)(4).

- The Act specifically exempts from its scope "personal data collected, processed, sold, or disclosed in compliance with the Federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.)." Conn. Pub. Act No. 22-15 § 3(b)(12).

Delaware Personal Data Privacy Act, effective January 1, 2025.

- The DPDPA does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined to mean "any information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information." H.B. 154, 152nd Gen. Assemb. §12D-102(21) (Del. 2023).

- "Sensitive data" means personal data that, among other things, includes "precise geolocation data." H.B. 154, 152nd Gen. Assemb. §12D-102(30)(d) (Del. 2023).

"Precise geolocation data" means "information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet." H.B. 154, 152nd Gen. Assemb. §12D-102(22) (Del. 2023).

- The DPDPA restricts the collection of personal data to what is "reasonably necessary" within the purpose disclosed to the consumer, and restricts processing of such information to purposes that are "reasonably necessary," absent consumer consent. H.B. 154, 152nd Gen. Assemb. §12D-106(a)(1), (2) (Del. 2023). Sensitive data may not be processed without consent. H.B. 154, 152nd Gen. Assemb. §12D-106(a)(4) (Del. 2023).

- Consumers have the right to obtain copies of their personal data in a reasonably accessible format within 45 days of a request, except that data "controllers" are not required to disclose trade secret information. Although not expressly included, this provision should give consumers a right to request and receive VPD in a readable format. H.B. 154, 152nd Gen. Assemb. §12D-104(a)(4), (c)(1) (Del. 2023)

- The DPDPA also covers "biometric data," defined as data "generated by automatic measurements of an individual's unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics can be used to identify a specific individual." H.B. 154, 152nd Gen. Assemb. § 12D-102(3) (Del. 2023). The definition excepts, however, photographs and certain recordings and certain data derived therefrom. Biometric data is included within the definition of "sensitive data." H.B. 154, 152nd Gen. Assemb. §12D-102(30)(b) (Del. 2023).

- The DPDPA specifically exempts from its scope "personal data collected, processed, sold, or in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended." H.B. 154, 152nd Gen. Assemb. §12D-103(8) (Del. 2023).

- In addition, the OCPA does not prohibit a controller or processor of personal data from collecting and retaining the data for internal use to "effectuating a product recall" or "conduct internal research to develop, improve or repair products, services or technology." H.B. 154, 152nd Gen. Assemb. §12D-110(b) (Del. 2023).

Iowa Consumer Data Protection Act of 2023, effective January 1, 2025.

- The Iowa Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined to mean "any information that is linked or reasonably linkable to an identified or identifiable natural person." It does not include "de-identified or aggregate data or publicly available information S.F. 262, 90th Gen. Assemb., Reg. Sess. § 1(18) (Iowa 2023). In addition, "sensitive data" is defined to include "precise geolocation data," and the Act restricts processing of such data without providing the consumer notice and an opportunity to opt out. S.F. 262, 90th Gen. Assemb., Reg. Sess. §§ 1(26)(d), 4(2) (Iowa 2023).

- The Act also covers "biometric data," defined as "data generated by the automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." S.F. 262, 90th Gen. Assemb., Reg. Sess. § 1(4) (Iowa 2023). Such data also is included within the definition of "sensitive data" when it is "processed for the purpose of uniquely identifying a natural person." S.F. 262, 90th Gen. Assemb., Reg. Sess. § 1(26)(b) (Iowa 2023). While this may not have obvious implications in a discussion about VPD, recent litigation in Illinois involving Subaru's driver monitoring feature suggests otherwise.

- The Act specifically exempts from its scope "personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq." S.F. 262, 90th Gen. Assemb., Reg. Sess. § 2(3)(n) (Iowa 2023).

- In addition, the Act does not prohibit a controller of processor of protected data from collecting, using, or retaining data "to conduct internal research to develop, improve, or repair products, services, or technology" or to "effectuate a product recall." S.F. 262, 90th Gen. Assemb., Reg. Sess. § 7(2) (Iowa 2023).

Indiana Consumer Data Protection Act of 2023, effective January 1, 2026.

- The INCDPA does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined to mean "information that is linked or reasonably linkable to an identified or identifiable individual." It does not include "de-identified data," "aggregate data," or "publicly available information." S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 2, § 19 (Ind. 2023). "Sensitive data" is defined to include "precise geolocation data," which is "information derived from technology, including global positioning system level latitude and longitude coordinates, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty (1,750) feet." S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 2, §§ 20, 28 (Ind. 2023).

- The INCDPA restricts processing of any personal data without consumer notice and consent. S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 4, § 1(2) (Ind. 2023).

- The INCDPA also covers "biometric data," defined as data that "is generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, images of the retina or iris, or other unique biological patterns or characteristics" and "is used to identify a specific individual." S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 2, § 4 (Ind. 2023). Such data is included within the definition of "sensitive data" when it is "processed for the purpose of uniquely identifying a specific individual." S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 2, §§ 28(2) (Ind. 2023).

- The INCDPA specifically exempts from its scope "personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.)." S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 1, § 2(10) (Ind. 2023).

- In addition, the Act does not prohibit a controller or processor of protected data from collecting, using, or retaining data to "conduct internal research to develop, improve, or repair products, services, or technology" or to "effectuate a product recall." S.B. 5, 123rd Gen. Assemb., First Reg. Sess., Chap. 8, § 2(1)-(2) (Ind. 2023).

Kentucky Consumer Data Protection Act, effective January 1, 2026.

- The Kentucky CDPA does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as any information that is linked to an identified or identifiable natural person, and it does not include de-identified data or publicly available information. 24RS HB 15 § 1(19). "Sensitive data" is defined as a category of personal data that includes: personal data indicating racial or ethnic original, religious beliefs, mental or physical health diagnosis, or citizenship or immigration status; the processing of genetic or biometric data that is processed for the purpose of uniquely identifying a specific natural person; the personal data collected from a known child; or precise geolocation data. 24RS HB 15 § 1(29)(a-e).

- The Kentucky CDPA restricts the processing of personal data for purposes that are not "reasonably necessary" for the disclosed purposes that it is being processed without the consumer's consent. 24RS HB 15 § 4(1)(b).

- "Biometric data" is defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual." It does not include a photograph, video, or audio recording. 24RS HB 15 § 1(3).

- The bill also restricts a controller's or a processor's ability to collect data to "conduct internal research to develop, improve, or repair products, services, or technology." 24RS HB 15 § 8(2).

- Finally, the Kentucky CDPA specifically exempts from its scope data that is collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. sec. 2721 et seq. 24RS HB 15 § 2(3)(k).

Maryland Online Data Privacy Act, effective October 1, 2025.

- Maryland's Online Data Privacy Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as any information that is linked or can be reasonably linked to an identified or identifiable person. It does

not include de-identified data or publicly available information. S. B. 541 § 14-4601 (W)(1-2)(I-II) (MD. 2024). "Sensitive data" is defined to include any data that reveals race or ethnicity, religious beliefs, health information, sexual orientation, transgender or nonbinary status, citizenship or immigration status, biometric data, precise geolocation, and personal data of a known child. S. B. 541 § 14-4601 (GG)(1)(I-VII)-(GG)(4) (MD. 2024).

- The Act restricts the processing of personal data for a purpose that is not reasonably necessary with the disclosed purposes for which the data is process without the consumer's consent. S. B. 541 § 14-4607 (A)(8) (MD. 2024).

- Under the Act, "biometric data" is defined as data that is "generated by automatic measurements of the biological characteristics of a consumer that can be used to uniquely authenticate a consumer's identity." S. B. 541 § 14-4601 (D)(1) (MD. 2024). This can include fingerprints, voice prints, or eye retina or iris images.

- Maryland's Online Data Privacy Act exempts personal data collected or processed in compliance with the federal Driver's Privacy Protection Act of 1994. S. B. 541 § 14-4603 (B)(8) (MD. 2024).

- Under the Act does not restrict a controller's or processor's ability to collect, use, or retain personal data for internal use to effectuate a product recall, identify and repair technical errors, and perform internal operations. S. B. 541 § 14-4612 (B)(2)(I-III) (MD. 2024).

Minnesota Consumer Data Privacy Act, effective July 31, 2025.

- The Minnesota Consumer Data Privacy Act does not define "vehicle information" and does not include any provisions specific to VPD. "Personal data" is defines to mean "any information that is linked or reasonably linkable to an identified or identifiable natural person." It does not include deidentified data or publicly available information. H. F. 4757 Article 5, § 3. 352O.02 (p) (Minn. 2024). "Sensitive data" is defined to include personal data reveal race, ethnic origin, religious beliefs, mental or physical health conditions, sexual orientation, citizenship or immigration status, biometric data, and geolocation data. H. F. 4757 Article 5, § 3. 352O.02 (v)(1-4) (Minn. 2024).

- "Biometric data" is defined as data that is "generated by automatic measurements of an individual's biological characteristics, including a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual." It does not include photographs, audio or visual recordings. H. F. 4757 Article 5, § 3. 352O.02 (d)(1-2) (Minn. 2024).

- The Act exempts personal data collected or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, "if the collection, processing, sale or disclosure is in compliance with that law." H. F. 4757 Article 5, § 4. 352O.03 (a)(10) (Minn. 2024).

Montana Consumer Data Privacy Act, effective October 1, 2024.

- The MTCDPA does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined to mean "any information that is linked or reasonably linkable to an identified or identifiable individual." It does not include "de-identified data or publicly available information." S.B. 384, 68th Legis., Reg. Sess. § 2(15) (Mont. 2023). "Sensitive data" is defined to include "precise geolocation data," which is "information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet." S.B. 384, 68th Legis., Reg. Sess. § 2(16)(a), (24) (Mont. 2023).

- The MTCDPA restricts processing of any personal data without consumer notice and consent. S.B. 384, 68th Legis., Reg. Sess. § 7(2)(a)-(b), (24) (Mont. 2023).

- The MTCDPA also covers "biometric data," defined as data that "is generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual." S.B. 384, 68th Legis., Reg. Sess. § 2(3)(a) (Mont. 2023). Such data is included within the definition of "sensitive data" when it is processed for "the purpose of uniquely identifying an individual." S.B. 384, 68th Legis., Reg. Sess. § 2(24)(b) (Mont. 2023).

- The MTCDPA specifically exempts from its scope "personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq." S.B. 384, 68th Legis., Reg. Sess. § 4(2)(l) (Mont. 2023).

- In addition, the MTCDPA does not prohibit a controller or processor of protected data from collecting, using, or retaining data "for internal use to ... conduct internal research to develop, improve, or repair products, services, or technology" or to "effectuate a product recall." S.B. 384, 68th Legis., Reg. Sess. § 11(2)(a)-(b) (Mont. 2023).

Nebraska Data Privacy Act, effective January 1, 2025.

- The Nebraska Data Privacy Act does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as any information that is reasonably linked to an identifiable individual, and include pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identifiable individual. LB1074 § 1(20)(a-b) (NE 2024). "Sensitive data" is defined as data "revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status." It also includes biometric data, data collected from a known child, and precise geolocation data. LB1074 § 1(30)(a-d) (NE 2024).

- The NEDPA restricts the collection and processing of personal data to what is adequate and reasonably necessary to the purposes the data is processed as disclosed to the consumer. LB1074 § 12(1)(a) (NE 2024).

- The bill defines "biometric data" as "data that is generated to identify a specified individual through an automatic measurement of a biological characteristic of such individual," and it includes fingerprints, voiceprints, and retina and iris images. LB1074 § 1(3)(a)(i-iv) (NE 2024).

- The bill does not apply to "[p]ersonal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as such act existed on January 1, 2024." LB1074 § 4(12) (NE 2024).

New Hampshire Data Privacy Bill, SB 255, effective January 1, 2025.

- SB 255 does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined as any information that is linked or reasonably linkable to an identified or identifiable individual. It does not include "de-identified" data or publicly available information. S.B. 255-FN, 2024 Sess. § 507-H:1(XIX) (NH 2024). "Sensitive data" is defined as "data revealing racial or ethnic origins, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status." It also includes biometric data, data collected from a known child, or geolocation data. S.B. 255-FN, 2024 Sess. § 507-H:1(XXVIII) (NH 2024).

- The bill restricts the processing of personal data unless the controller obtains consumer's consent. S.B. 255-FN, 2024 Sess. § 507-H:4(I)(a)-(g) (NH 2024).

- The bill further defines "biometric data" as "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual." It does not include photographs, videos, or audio recordings, unless the data is generated to identify an individual. S.B. 255-FN, 2024 Sess. § 507-H:1(IV) (NH 2024).

- Additionally, the bill does not prohibit a controller or processor from using or retaining data for internal use to "[c]onduct internal research to develop, improve, or repair products, services, or technology," to "effectuate a product recall," or to "identify and repair technical errors that impair existing or intended functionality." S.B. 255-FN, 2024 Sess. § 507-H:10(II)(a)-(c) (NH 2024).

- SB 255 also specifically exempts from its scope "[p]ersonal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended." S.B. 255-FN, 2024 Sess. § 507-H:3(II)(l) (NH 2024).

New Jersey Data Privacy Act, effective January 15, 2025.

- The NJDPA does not specifically define "vehicle information" or include any provisions specific to VPD. However, the NJDPA does not apply to "the sale of a consumer's personal data by the New Jersey Motor Vehicle Commission that is permitted by the federal "Drivers' Privacy Protection Act of 1994." S.B. 332 §6(e) (NJ. 2024).

- The NJDPA defines "personal data" to mean "any information that is linked or reasonably linkable to an identified or identifiable person." It does not include "de-identified" data or publicly available information. "Sensitive data" is defined to mean "personal data revealing racial or ethnic origin; religious beliefs; mental or physical health condition, treatment, or diagnosis; financial information, or credit or debit card number,…,genetic or biometric data that may be processed or for the purpose of uniquely identifying an individual; personal data collected from a known child, or precise geolocation." It also includes sexual orientation, citizenship status, and transgender or non-binary status. S.B. 332 §1 (NJ. 2024).

- It further defines "biometric data" to mean "data generated by automatic or technological processing, measurements, or analysis of an individual's biological, physical, or behavioral characteristics…that are used or intended to be used…to identify a specific individual." It does not include photographs, videos, or audio recordings unless the data is generated to identify an individual. S.B. 332 §5(11)(1) (NJ. 2024).

- A controller cannot process personal data for reasons that are not considered necessary without the consumer's consent. S.B. 332 §5(9) (NJ. 2024).

- Nothing in the NJDPA shall apply to "an insurance institution subject to P.L.198,c179 (C.17:23A-1 et seq.)."

Oregon Consumer Privacy Act, effective July 1, 2024.

- The OCPA does not specifically define "vehicle information" or include any provisions specific to VPD. "Personal data" is defined to mean "data, derived data or any unique identifier that is linked to or is reasonably linkable to a consumer or to a device that identifies, is linked to or is reasonably linkable to one or more consumers in a household." It does not include "de-identified data" or certain "lawfully available" data as identified in the Act. S.B. 619-B, 82nd Legis., Reg. Sess. § 1(13) (Or. 2023). "Sensitive data" is defined to include personal data that "accurately identifies within a radius of 1,750 feet a consumer's present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology that includes, but is not limited to, a global positioning system that provides latitude and longitude coordinates." S.B. 619-B, 82nd Legis., Reg. Sess. § 1(18)(a)(C) (Or. 2023).

- The OCPA restricts the processing of any personal data that is "not reasonably necessary for and compatible with" specified purposes without consumer notice and consent. S.B.

619-B, 82nd Legis., Reg. Sess. § 5(2)(a) (Or. 2023). Sensitive data may not be processed without consent. S.B. 619-B, 82nd Legis., Reg. Sess. § 5(2)(b) (Or. 2023).

- The OCPA also covers "biometric data," defined as data that "is generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer." S.B. 619-B, 82nd Legis., Reg. Sess. § 1(3) (Or. 2023). The definition excepts, however, photographs and certain recordings, certain data derived therefrom, and certain facial mapping. Biometric data is included within the definition of "sensitive data." S.B. 619-B, 82nd Legis., Reg. Sess. § 1(18) (Or. 2023).

- The OCPA specifically exempts from its scope "information collected, processed, sold, or disclosed under and in accordance with" the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 *et seq*. S.B. 619-B, 82nd Legis., Reg. Sess. § 2(2)(k)(B) (Or. 2023).

- In addition, the OCPA does not prohibit a controller or processor of personal data from "effectuating a product recall" or from "conducting internal research to develop, improve or repair products, services or technology." S.B. 619-B, 82nd Legis., Reg. Sess. § 2(3)(j)-(k) (Or. 2023).

- The OCPA expressly exempts insurers from its scope. S.B. 619-B, 82nd Legis., Reg. Sess. § 2(2)(n) (Or. 2023).

Rhode Island Data Transparency and Privacy Protection Act, effective January 1, 2026.

- The Rhode Island Data Transparency and Privacy Protection Act ("the Rhode Island Data Privacy Act") was signed into law on June 28, 2024. It does not specifically define "vehicle information" or include any provisions specific to VPD. The Act defines "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable individual and does not include de-identified data or publicly available information." S. 2500, Gen. Assemb., Jan. Sess § 6-48.1-2.(18) (RI 2024).

- "Sensitive data" is defined as personal data that does include data that reveals racial or ethnic origin, religious beliefs, mental or physical health conditions, sex life, sexual orientation, or immigration status, or data that uniquely identifies an individual or precise geolocation. S. 2500, Gen. Assemb., Jan. Sess. § 6-48.1-2.(26) (RI 2024).

- Controllers are required to obtain customer consent before processing any sensitive data concerning a customer and shall not process the sensitive data of a known child unless consent is obtained in accordance with COPPA. S. 2500, Gen. Assemb., Jan. Sess. § 6-48.1-4.(c) (RI 2024).

- The Act defines "biometric data" as data that is "generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint," eye retina or iris pattern, or other characteristics that are used to identify a specific individual. It

does not include photographs, video or audio recordings, unless that data is generated with the purpose to identify a specific individual. S. 2500, Gen. Assemb., Jan. Sess § 6-48.1-2.(3) (RI 2024).

- Specifically exempt from the Act is personal data that is collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, U.S.C. § 2721 et seq., as amended from time to time. S. 2500, Gen. Assemb., Jan. Sess. § 6-48.1-3.(e)(12) (RI 2024).

Tennessee Information Protection Act, effective July 1, 2024.

- The TIPA does not specifically define "vehicle information" or include any provisions specific to VPD. It defines "personal information" as "information that identifies, relates to, or describes a particular consumer or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer." Such information includes identifiers such as name, SSN, and driver license number; associative information like addresses and insurance policy numbers; commercial information like purchases made; biometric data; "electronic network activity;" geolocation data; etc. It does not include information that is "publicly available" or "de-identified or aggregate consumer information." H.B. 1181, 113th Gen. Assemb., Reg. Sess. § 47-18-3201(16) (Tenn. 2023).

- In addition, "sensitive data" is defined as personal information that includes, among other things, "precise geolocation data," which is "information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750')." H.B. 1181, 113th Gen. Assemb., Reg. Sess. § 47-18-3201(17), (25) (Tenn. 2023).

- The TIPA restricts processing of any personal data without consumer notice and consent. H.B. 1181, 113th Gen. Assemb., Reg. Sess., Part 47-18-3204(a) (Tenn. 2023).

- The TIPA also covers "biometric data," defined as data that is "generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual." H.B. 1181, 113th Gen. Assemb., Reg. Sess. § 47-18-3201(3) (Tenn. 2023). Such data is included within the definition of "sensitive data" when it is processed for "the purpose of uniquely identifying a natural person." H.B. 1181, 113th Gen. Assemb., Reg. Sess., Part 47-18-3201(25)(B) (Tenn. 2023).

- The TIPA specifically exempts from its scope "personal information collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.)." H.B. 1181, 113th Gen. Assemb., Reg. Sess., Part 47-18-3210(a)(17) (Tenn. 2023).

- In addition, the TIPA does not prohibit a controller of processor of protected data from collecting, using, or retaining data to "conduct internal research to develop, improve, or repair products, services, or technology" or to "effectuate a product recall." H.B. 1181, 113th Gen. Assemb., Reg. Sess., Part 47-18-3208(b) (Tenn. 2023).

Texas Data Privacy and Security Act, effective July 1, 2024.

- The TDPSA does not specifically define "vehicle information" or include any provisions specific to VPD. It defines "personal data" as "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual." Notably, the definition of "personal data" expressly "includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual." However, it does not include "deidentified data or publicly available information." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.001(19) (Tex. 2023).

- "Sensitive data" is defined as "a category of personal data" that includes, among other things, "precise geolocation data," which is "information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet (1,750')." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.001(21), (29)(C) (Tex. 2023).

- If a consumer "provides" data to a controller and such data is available in "a digital format," the controller must provide such data to the consumer following an "authenticated request" in a "readily usable format that allows the consumer to transmit the data to another controller without hindrance." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.051(b)(4) (Tex. 2023). With some exceptions, the controller also must respond to the request free of charge and within 45 days. H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.052(b), (d) (Tex. 2023).

- The TDPSA restricts the processing of personal data for undisclosed purposes without consumer consent, and the processing of sensitive data without consent. H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.101 (Tex. 2023).

- The TDPSA also covers "biometric data," defined as data that is "generated by automatic measurement of an individual's biological characteristics," including "a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.001(3) (Tex. 2023). Such data is included within the definition of "sensitive data" when it is "processed for the purpose of uniquely identifying an individual." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.001(29)(B) (Tex. 2023).

- The TDPSA specifically exempts from its scope "personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994 (18

U.S.C. Section 2721 et seq.)." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.003(12) (Tex. 2023).

- In addition, the TDPSA does not prohibit a controller of processor of protected data from collecting, using, or retaining data to "conduct internal research to develop, improve, or repair products, services, or technology" or to "effect a product recall." H.B. 4, 88th Gen. Assemb., Reg. Sess. § 541.202 (Tex. 2023).

For more information on the general data protections afforded by each of these state laws (not specific to VPD), see Schedule A, attached.

* * *

In addition to the five state consumer data privacy laws, the Illinois Biometric Information Privacy Act ("BIPA") has unique implications for drivers and others with interest in connected vehicle data, as illustrated most recently in the putative class action pending against Subaru of America for alleged violations of BIPA through its processing of drivers' biometric identifiers in connection with its driver monitoring system (ostensibly, a safety feature).

Enacted in 2008, BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." BIPA highlights the importance of protecting this information by explaining that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." Under BIPA, entities that use and store biometric identifiers must comply with certain notice and consent requirements.

SCHEDULE A

A. Virginia's Consumer Data Protection Act ("CDPA")

Under the CDPA, obligations are imposed on entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that either:

- Control or process the personal data of at least 100,000 consumers during a calendar year.

- Control or process the personal data of at least 25,000 consumers and derive at least 50% of its gross revenue from the sale of personal data.

Consumer Rights

1. **Right to access.** Consumers have the right "to confirm whether or not a controller is processing the consumer's personal data and to access such personal data."

2. **Right to correct.** Consumers have the right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data.

3. **Right to delete.** Consumers have the right to delete personal data provided by or obtained about the consumer.

4. **Right to data portability.** Consumers have the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

5. **Right to opt out.** To opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data and profiling in advancing decisions that produce legal or similarly significant effects concerning the consumer.

6. **Right to appeal.** The final right the CDPA provides to consumers is the right to appeal a business's denial to act within a reasonable time. Under the law, a business must respond to a consumer request within 45 days of receipt of the request. Where reasonably necessary, the business may then extend the response deadline by an additional 45 days as long as they notify the consumer within the initial response window. If a business fails to do this, the CDPA mandates that a "controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable time after the consumer's receipt of the decision." If the appeal is denied, the controller needs to inform the consumer how they can submit a complaint to the attorney general.

Businesses Obligations

1. **Limits on collection.** The CDPA includes a provision limiting the collection of data to that which is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed."

2. **Limits on use.** Once the data has been collected, the statute mandates a business "not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent." Furthermore, the act imposes limits on processing sensitive personal information such that doing so is prohibited absent consumer consent.

3. **Technical safeguards.** In addition to imposing obligations on the business's processing activities, the CDPA also mandates a business "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."

4. **Data protection assessments.** The CDPA also requires controllers to conduct "data protection assessments" that evaluate the risks associated with processing activities. While the act specifies the types of activities that must be assessed, it fails to indicate how often they must occur and how long they must be kept.

5. **Data processing agreements.** The CDPA requires that processing activities undertaken by a processor on behalf of a controller be governed by a data processing agreement. Such agreements must "clearly 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." The provision provides a set of enumerated terms that must be included in the agreement.

6. **Privacy policy.** The CDPA contains a provision requiring controllers to provide consumers with a privacy policy. The policy must state:

- The categories of personal data processed by the controller.
- The purpose for processing personal data.
- How consumers may exercise their consumer rights and appeal a controller's decision regarding the consumer's request.
- The categories of personal data that the controller shares with third parties, if any.
- The categories of third parties, if any, with whom the controller shares personal data.

The CDPA has no requirements regarding the time disclosures must be made or any particular format they must follow.

Access Requests. Controllers are required to establish and describe in a privacy notice one or more secure and reliable means for consumers to submit a request to exercise their rights. The method used needs to consider how consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the requests. Controllers are prohibited from requiring a consumer to create a new account in order to exercise their consumer rights but may require a consumer to use an existing account.

45 days to respond. Controllers are required to respond to consumer requests within 45 days. This time period may be extended once by 45 additional days if certain requirements are met.

No charge for information. Controllers are required to provide information in response to a consumer request free of charge, up to twice annually per consumer. The controller may charge the consumer a reasonable fee or decline to act on the request if requests are manifestly unfounded, excessive or repetitive, but the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request is on the controller.

Justification for failure to act. If a controller declines to act regarding the consumer's request, the controller shall inform the consumer why within 45 days and provide instructions for how to appeal the decision.

Denial of requests. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action and may request additional information reasonably necessary to authenticate the consumer and the consumer's request.

Right to appeal. A controller is required to establish a process for a consumer to appeal its refusal to act on a request, and if the appeal is denied, an online mechanism or other method for the consumer to contact the attorney general to submit a complaint.

B. California Consumer Privacy Act ("CCPA")

The CCPA defines a "business" subject to CCPA as a for-profit entity doing business in California that collects or processes consumers' personal information and meets one or more of these thresholds:

- Annual gross revenues in excess of $25,000,000.
- Annually buys, receives, sells or shares 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.

Consumer Rights

1. **Right to Know** what personal information is collected.

2. **Right to Access** personal information.

3. **Right to Know if Personal Information is Sold.**

4. **Right to Delete**. Unless the personal information is necessary for the business or service provider to maintain the consumer's personal information in order to do a variety of things, including but not limited to completing transactions, detecting security threats, exercise free speech, comply with a legal obligation or internal use in a lawful manner.

5. **Right to Data Portability**. Section 1798.100(d), Section 130(a)(2).

6. **Right to Opt Out of Sale**.

Businesses Obligations

1. **Opt-out methods**. A business that sells personal information about consumers to third parties is required to provide a clear and conspicuous link on its internet homepage titled "Do Not Sell My Personal Information" to a webpage that enables a consumer to opt out of the sale. A business is prohibited from requiring a consumer to create an account to opt out.

2. **Purpose Limitation**. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing notice.

3. **Reasonable security Procedures**. Business must implement and maintain reasonable security procedures and practices.

4. **Required Notices**. Notices are required at collection, notice of right to opt-out, and notice of financial incentive.

5. **Privacy Notice Required**. Businesses must provide a privacy policy.

6. **No discrimination**. Business are prohibited from discriminating against consumers for exercising their rights.

Submitting Requests. Businesses need to make available to consumers two or more designated methods for submitting requests for information, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests. The business may require authentication of the consumer but shall not require the consumer to create an account with the business to make a verifiable consumer request. If the consumer has an account with the business, the consumer may be required to use that account to submit a request.

45 days to respond. Businesses are required to disclose and deliver the required information to a consumer within 45 days of receiving a verifiable consumer request. This time period may be

extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

No charge for information. The business must deliver the requested information free of charge. If requests from a consumer are manifestly unfounded or excessive, a business may either charge a reasonable fee or refuse to act on the request. The business shall bear the burden of demonstrating any verified consumer request is manifestly unfounded or excessive.

Inform consumer why no action. If the business does not act on the consumer's request, it shall inform the consumer of its reasons and any rights the consumer may have to appeal the decision to the business.

C. California Privacy Rights Act ("CPRA")

*Effective Dec. 16, 2020. Most provisions are not operative until Jan. 1, 2023. Provisions operative now include certain exemptions, the Regulations provisions, and certain provision regarding the California Privacy Protection Agency. Enforcement begins July 1, 2023.

A business subject to the CPRA is a for-profit entity doing business in California that collects or processes consumers' personal information and meets one of these thresholds:

- Annual gross revenues in excess of $25,000,000 in the preceding calendar year.
- Annually buys, sells or shares the personal information of 100,000 or more consumers or households.
- Derives 50% or more of its annual revenues from selling or sharing consumers' personal information.

Consumer Rights

1. **Right to Know what Personal Information is Being Collected and Right to Access** personal information.
2. **Right to Know what Personal Information is Sold or Shared and to Whom.**
3. **Right to Correct.**
4. **Right to Delete.** (Subject to certain exceptions).
5. **Right to Data Portability.**
6. **Right to Opt Out of Sale or Sharing**. Definition of sharing includes "cross-context behavioral advertising," a separately defined term.
7. **Right to Limit Use and Disclosure of Sensitive Personal Information.**

The CPRA generally expands on or modifies the existing CCPA rights.

Businesses Obligations

1. **Methods of Limiting Sale, Sharing and Use of Personal Information and Sensitive Personal Information.** A business that sells or shares personal information or uses or discloses sensitive personal information for purposes other than those authorized by 1798.121(a) is required to:

- Provide a clear and conspicuous link on its internet homepage titled "Do Not Sell or Share My Personal Information" to a webpage that enables a consumer to opt-out of the sale or sharing.

- Provide a clear and conspicuous link on its internet homepage titled "Limit the Use of My Sensitive Personal Information" that enables a consumer to limit the use or disclosure of the consumer's sensitive personal information.

A business can use one link to opt out of the sale or sharing and limit the use of sensitive personal information. A business is prohibited from requiring a consumer to create an account to opt out or limit the use of sensitive personal information.

2. **Data Minimization.** Prohibits a business from retaining a consumer's personal information or sensitive personal information for longer than is reasonably necessary for that disclosed purpose.

3. **Purpose Limitation.** Requires that a business's collection, use, retention and sharing of a consumer's personal information be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected.

4. **Reasonable Security Procedures**. A business that collects a consumer's personal information is required to implement reasonable security procedures and practices in accordance with Section 1798.81.5. Also Section 1798.150, the Private Right of Action provision, references a business' duty to implement and maintain reasonable security procedures and practices.

5. **Sensitive Data**. A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information is prohibited from doing so.

6. **Required Notices**. Section 1798.100, notice at collection, broadened to include sensitive personal information and retention information; Section 1798.120, notice of right to opt out of sale and sharing; Section 1798.121, notice regarding sensitive personal information required under certain circumstances; Section 1798.125, notice of financial incentive. Section 1798.130(a)(5) requires certain information be disclosed in a business's online privacy policy and in any California-specific description of consumer's privacy rights or on its website, including a description of a consumer's rights and two or more methods for submitting requests, as well as disclosures required by Sections 1798.110 and 1798.115.

7. **No Discrimination.** Businesses are prohibited from discriminating against consumers for exercising their rights. Businesses are permitted to offer financial incentives for the collection, sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.

Consumers are entitled to notice of any financial incentives and a business may enter a consumer into a financial incentive program only if the consumer gives prior opt-in consent. If a consumer refuses to provide opt-in consent, then the business must wait at least 12 months before next requesting opt-in consent.

Notice, Disclosure, Correction and Deletion Requirements. Make available to consumers two or more designated methods for submitting requests for information or requests for deletion or correction, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests. The business may require authentication of the consumer, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer has an account with the business, it may require the consumer to use that account to submit a request.

45 days to respond. Businesses are required to disclose and deliver the required information to a consumer, correct inaccurate personal information or delete a consumer's personal information within 45 days of receiving a verifiable consumer request. This time period may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

No charge for information. The business must deliver the requested information free of charge. If requests from a consumer are manifestly unfounded or excessive, a business may either charge a reasonable fee or refuse to act on the request. The business shall bear the burden of demonstrating any verifiable consumer request is manifestly unfounded or excessive.

Inform consumer why no action. If the business does not act on the consumer's request, the business shall inform the consumer of its reasons and any rights the consumer may have to appeal the decision to the business.

D. Colorado Privacy Act ("CPA")

The CPA applies to any controller that: "Conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and

- controls or processes the personal data of at least 100,000 consumers or more during a calendar year; or
- derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more."

Consumer Rights

1. **Right of access**. A consumer has the right to confirm whether a controller is processing Personal data concerning the consumer and to access such data.

2. **Right to Correction**.

3. **Right to Deletion**.

4. **Right to Data Portability**.

5. **Right to Opt out** of targeted advertising, the sale of personal data, or profiling via a universal opt-out mechanism.

Controller Obligations

1. **Duty of Data Minimization**. A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.

2. **Duty of Purpose Specification**. A controller shall specify the express purposes for which personal data are collected and processed.

3. **Duty to avoid secondary use**. A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.

4. **Duty of Care**. A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition.

5. **Duty regarding sensitive data**. A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent.

6. **Duty of Transparency** (Privacy Notice). Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: (1) the categories of personal data collected or processed by a controller or processor; (2) the purposes for which the categories of personal data are processed; (3) how and where consumers may exercise their rights; (4) the categories of personal data that the controller shares with third parties and; (5) the categories of third parties with whom the controller shares personal data.

7. **Required disclosure of sale**. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may opt out.

8. **Duty to avoid unlawful discrimination**. A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

Access Requests. Consumers may exercise their rights by submitting a request using a method specified by the controller in the required privacy notice. The method must take into account: (1) the ways in which consumers normally interact with the controller; (2) the need for secure and reliable communication relating to the request; and (3) the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights. However, a controller may require a consumer to use an existing account.

45 days to respond. A Controller shall inform a consumer of any action taken on a request within 45 days. In certain circumstances, this 45-day window to respond may be extended by an additional 45 days.

No charge for information. Controllers are required to provide the information requested free of charge once per year. For additional requests within a 12-month period, the controller may charge an additional amount.

Justification for failure to act. If a controller does not take action as requested by a consumer, the controller shall inform the consumer within 45 days after receipt of request of the reasons for not taking action and instructions for how to appeal the decision.

Denial of requests. A controller is not required to comply with a request to exercise any of the consumer's rights if the controller is unable to authenticate the request using commercially reasonable efforts and may request the provision of additional information reasonably necessary to authenticate the request.

Right to appeal. A controller shall establish an internal process whereby consumers may appeal a refusal to take action on a consumer request. Where a consumer wishes to appeal, they must do so within a reasonable time period after the controller notifies them that the controller is denying the request. The appeal process must be conspicuously available and easy to use.

E. Utah Consumer Privacy Act

On March 25, 2022, Utah enacted the Utah Consumer Privacy Act ("UCPA"), becoming the fourth state to enact consumer data privacy legislation, which will go into effect on December 31, 2023. The UCPA establishes obligations for businesses on the handling and processing of personal data of Utah consumers, while also giving Utah consumers certain rights over data that is given to the businesses. The UCPA is most similar to the Virginia Consumer Data Privacy Act and the Colorado Privacy Act, other than that the UCPA is only applicable to businesses with an annual revenue of at least $25 million and, unlike the others, it does not have a data protection assessment requirement. In general, the UCPA is more "business-friendly" than the VCDPA, the Colorado Privacy Act, and the CCPA.

The UCPA applies to any controller or processor who:

- Conducts business in the state or produces a product or service that is targeted to consumers who are residents of the state;
- Has annual revenue of $25 million or more; and

- Satisfies one or more of the following:
    - During a calendar year, controls or processes personal data of 100,000 or more consumers; or
    - Derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

Consumer Rights

1. Right to Know and "to confirm whether a controller is processing the consumer's personal data."

2. Right to Access their personal data.

3. Right to Delete the consumer's personal data that was provided to the controller.

4. Right to a Copy. Consumers have the right to contain a copy of the personal data that has been provided to the controller by the consumer in a portable and readily usable format.

5. Right to Opt Out of the processing of personal data for the purposes of targeted advertising and sale of that personal data.

6. Right to Avoid Discrimination. A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

Controller Obligations:

1. Duty of Transparency and Purpose Specification. The UCPA requires a controller to provide a reasonably clear privacy notice to consumer that includes all of the categories of personal data being collected, the intended purpose of that data, how consumers can exercise their rights, and what categories are being shared to third parties.

2. Duty regarding sensitive. The UCPA does not require opt-in consent, but controllers must provide consumers notice and an opportunity to opt out before processing sensitive data.

3. Duty of Security. Controllers must establish and maintain administrative, technical, and physical security practices to guard the confidentiality of personal data, considering foreseeable risks to consumers related to the processing of sensitive data.

4. Duty to avoid unlawful discrimination. A controller cannot deny a good or service, charge a different rate or provide a different level of quality to a consumer.

5. **Provision of products and services.** Under the UCPA, the controller does not have to provide a product or service to a consumer if personal data is required and the consumer has not consented to the process of their personal data.

Privacy Notice. Controllers must provide consumers with a "reasonably accessible and clear privacy notice," including all of the categories of personal that that will be collected and processed, the purpose that the data is being collected, and which third parties will be able to access that data. If personal data is being sold to third parties for targeted advertising, the controller must disclose that activity to the consumer.

45 days to respond. A controller shall inform a consumer of any action taken on a request within 45 days. In certain circumstances, this 45-day window to respond may be extended by an additional 45 days.

Enforcement. While the UCPA does not include a private right to action, the Utah Attorney General and the Utah Department of Commerce Division of Consumer Protection are tasked with investigating consumer complaints, and must compile and submit an enforcement report to the Business and Labor Interim Committee by July 1, 2025, evaluating the liability and enforcement provisions of the UCPA.

F. Connecticut Data Privacy Act ("CTDPA")

Effective July 1, 2023, this Connecticut act establishes personal data protection standards and responsibilities, and gives consumers the right to "access, correct, delete and obtain a copy of personal data, and opt out of the processing of personal data." The CTDPA applies to service provides that maintain personal data on behalf of businesses and also Connecticut residents who process the personal data of:

- at least 100,000 consumers or more annually, except personal data controlled or processed for the purpose of completing a payment transaction; or
- 25,000 or more consumers and derived over 25% of gross revenue from the sale of personal data.

Consumer Rights

1. **Right to access** personal data that is collected, unless such actions would reveal a trade secret.
2. **Right to Correction.**
3. **Right to Deletion.**
4. **Right to Data Portability.**
5. **Right to Opt-Out** of targeted advertising, the sale of personal data, or profiling in advancing decisions that produce legal or similarly significant effecs concerning the consumer.

Controller Obligations

1. Duty of Transparency and Purpose Specification. The CTDPA requires controllers to provide consumers with a reasonably clear privacy notice that includes categories of personal data collected, the purpose of the data collection, instructions for consumers to exercise their rights regarding their data, what data is shared with third parties, and a contact method for the controller.

2. Duty of Data Minimization. A controller's collection of personal data must be adequate, relevant, and reasonably necessary in relation to the specified purposes for which the data is processed.

3. Duty to avoid secondary use. A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the disclosed purposes for which such personal data is processed, unless the controller first obtains the consumer's consent.

4. Duty regarding sensitive data. A controller must obtain a consumer's consent before processing that consumer's personal data.

5. Duty of Security. Controllers must establish and maintain administrative, technical, and physical security practices to protect the confidentiality and accessibility of the personal data collected, taking into account the volume and nature of the personal data.

6. Duty to avoid unlawful discrimination. A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

7. Data protection assessments. The CTDPA requires controllers to conduct a data protection assessment for processing activities that present a "heightened risk of harm to a consumer, including processing personal data for targeted advertising, selling personal data, processing sensitive data, or processing personal data for profiling where it involves foreseeable risk.

8. Duty of revocable consent. The controller must provide the consumer with an effective method to revoke consent that is as easy as the method to provide consent. Once consent is revoked, the controller must cease processing data "as soon as practicable but no later than 15 days after receipt of the request."

G. Iowa Consumer Data Protection Act ("ICDPA")

On March 29, 2023, Iowa signed Senate File 262, the Iowa Consumer Data Protection Act (ICDPA), becoming the sixth state to enact a statewide consumer data privacy law. This law will go into effect on January 1, 2025, and will apply to any person doing business in Iowa, producing products largely targeted to Iowa consumers, and that process the data of:

- 100,000 Iowa consumers; or

- 25,000 Iowa consumers, if the entity derives over 50% of gross revenue from the sale of personal data.

Consumer Rights

1. Right to Confirm whether a controller is processing personal data and its access to personal data.

2. Right to Delete personal data. This right is limited to data obtained from the consumer.

3. Right to Request a copy of their personal data in a readily usable format.

4. Right to Opt Out of the sale of personal data. However, unlike the other state privacy laws, ICDPA does not explicitly provide consumers the right to opt of the use of their personal data for targeted advertising.

Unlike other state privacy laws, consumers do not have a right to correct any inaccuracies in their personal data information. Additionally, the law does not include any data protection or risk assessment requirements.

Controller Obligations

1. Controllers must implement reasonable technical and physical data security measures.

2. Controllers must process consumers' non-exempt sensitive data (such as genetic or biometric data, data regarding minors, or personal information) only after providing the consumer clear notice and opportunity to opt out.

3. Controllers must process consumer data in a non-discriminatory manner.

4. Controllers must create a process for consumers to appeal the refusal to take action on requests to exercise their rights.

5. Controllers must provide consumers a clear privacy policy that includes all of the categories or data being processed, as well as the purposes for processing that data, and the categories of data that is being shared to third parties. Consumer's rights regarding their data must also be included in the privacy policy.

6. Controllers must inform consumers if personal data is sold to third parties, and provide consumers an opportunity to opt out.

Privacy Notice. Iowa entities are encouraged to consider revising privacy policies to accurately reflect the processing of personal data and communicate any new or updated rights available to consumers, as well as the means for consumers to exercise those rights. These entities should also provide an appeal process for consumers, similar to the process required in Virginia.

Investigations and Enforcement. The Iowa Attorney General has the authority to conduct enforcement actions, issue investigative demands and impose sanctions. The ICDPA allows for a 90-day cure period for alleged violations, after which the entity or controller who continues to violate the law may be subject to an injunction or civil penalties of up to $7,500 per violation.

Controllers and Service Providers Agreement. Iowa requires controllers and data processors to enter into contracts that regulate how processors process data with clear instructions for the process, the nature and purpose of processing, and the type of data being processed. These contracts must also include a confidentiality agreement required for processors' agents or subcontractors. Like the VCDPA and CPA, the Iowa Data Privacy Law requires processors to delete or return personal data upon the controller's request.

ICDPA Compliance Checklist

- Confirm that your business is subject to the ICDPA.
- Create and revise a privacy policy.
- Implement "reasonable" security practices.
- Enable consumers to opt out of the sale of personal data when applicable.
- Provide notice to consumers for collecting sensitive data and implement opt-out opportunity.
- Develop receipt and response to consumer rights requests.
- Implement training for employees who are responsible for handling consumer rights requests.

H. Indiana Consumer Data Protection Act of 2023 ("INCDPA")

Indiana became the seventh state to pass a data privacy law, which goes into effect on January 1, 2026. The INCDPA most similarly resembles Virginia's VCDPA. The INCDPA applies to companies and entities conducting business in Indiana or selling products or services targeted to Indiana residents that either:

- control or process personal data of at least 100,000 Indiana residents during a calendar; or
- control or process personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal data.

Consumer Rights

1. **Right to Access** their personal data.
2. **Right to Correct** any inaccuracies or discrepancies in their personal data.

3. **Right to Delete** personal data. This right is limited to data obtained directly from the consumer.

4. **Right to Obtain** a copy of their personal data in a readily usable format. Controllers must respond to these requests within 45 days and must offer the right to appeal an adverse decision.

5. **Right to Opt-Out** of the sale of personal data and opt out of the use of their personal data for targeted advertising and profiling.

The most notable difference of the INCDPA compared to other state data privacy laws is the limitation of a consumer's right to correct, applying only to data that the consumer provided to the controller, not all personal data that is collected and processed by the controller. Additionally, the INCDPA has a very narrow definition of the term "sale," defined as an exchange of personal data for monetary consideration *only*.

Controller Obligations

1. A controller must limit the collection of personal data to what is reasonably necessary for purposes for which the data is being collected.

2. A controller must receive a consumer's express consent prior to processing the data for a purpose that is not reasonably necessary.

3. Controllers cannot discriminate against consumers for exercising their rights under the INCDPA. However, controllers may offer different prices, rates, levels, or quality or selection of goods or services to consumers if a consumer has voluntarily opted-in to the sale of personal data through a loyalty or rewards. program.

4. A controller may only process a consumer's personal data after receiving express consent from the consumer.

5. A controller must establish a privacy notice with at least one way for consumers to exercise their data rights.

Privacy Notices. Controllers must establish a clear privacy policy that outlines the categories of personal data being processed, as well as the purpose for processing that data. The notice must also include what categories of what are being shared with which third parties, as well as consumer's rights and in what manner consumers can exercise their rights.

Processor Contracts. The INCDPA requires controllers to enter a contract with data processors that regulate how processors are processing personal data. The law requires that instructions for data processing is clear and includes the nature and purpose for processing, as well as the categories of data, the duration of processing, and each parties' rights and obligations.

Investigations and Enforcement. The Indiana Attorney General has the authority to issue investigative demands for alleged violations. Under the INCDPA, controllers are given a 30-day

cure period for violations; controllers who continue to violate the law after the cure period will be subject to civil penalties of up to $7,500 per violation.

I. Montana Consumer Data Privacy Act ("MTCDPA")

On May 19, 2023, Montana's state legislature unanimously passed the Montana Consumer Data Privacy Act, becoming the ninth state to enact a comprehensive privacy law. The MTCDPA will go into effect on October 1, 2024. The MTCDPA is applicable to companies and entities that do business in Montana or target products or services to Montana consumers, and that:

- control or process personal data of 50,000 or more Montana consumers; or
- control or process personal data of 25,000 or more Montana consumers and derive over 25% of gross revenue from the sale of that data.

Of the nine state data privacy laws that have been enacted, the MTCDPA has the lowest applicability threshold, with most other data applying to businesses that process personal data of 100,000 residents due to the smaller population of the state.

The MTCDPA most closely resembles the Connecticut Data Privacy Act in that it provides consumers the right to revoke consent to the processing of their data, requiring businesses to provide universal means for opting out of the sale of personal data and targeted advertising, and that is permits consumers to request all of their personal data to be deleted, not just data a business or entity collected directly from the consumer.

Consumer Rights

1. **Right to Confirm** the processing of personal data.
2. **Right to Access** their personal information.
3. **Right to Correct** any inaccuracies in their personal information.
4. **Right to Delete** personal data provided by the consumer or obtained by a controller.
5. **Right to Request** a copy of their personal information held about them in a portable and usable form.
6. **Right to Opt-Out** of the sale of personal information, targeted advertising and profiling through automated means.
7. **Right to Appeal** any denial of a consumer request relating to the above rights.

Controllers must respond to consumer requests for their data within 45 days of the request and must offer the consumer the right to appeal. If a consumer appeals, the controller must respond

within 60 days. If controllers deny the appeal, controllers must also provide the consumer a method for contacting the Attorney General.

Controller Obligations

1. A controller must limit the collection of personal data to what is reasonably necessary for purposes for which the data is being collected.

2. A controller must acquire a consumer's consent in order to process or use personal data that is not for the purposes in which it was originally collected.

3. A controller must provide consumers an effective way to revoke consent for processing of personal data, and if consent is revoked, the controller must cease the processing of that data no later than 45 days after receipt of the request.

4. A controller cannot discriminate against consumers for exercising their rights under the MTCDPA. However, controllers may offer different rates, prices, quality or selection of goods or services if a consumer has exercised his/her rights to opt-in to the sale of personal data through voluntary consumer participation in loyalty or rewards programs.

5. A controller must provide a reasonably clear privacy notice that includes the categories of personal data being collected, the reasons for processing that data, what data is being shared to which third parties, and that outlines how consumers may exercise their consumer rights.

Processor Contracts. Controllers and processors contractual agreements must include allowing and cooperating with reasonable assessments of the processor by the controller or its agent.

Enforcement. The MTCDPA is enforceable by the Montana state attorney general's office. Entities found in violation of the law will be granted a 60-day cure period. If a controller cures the violation and provides the attorney general with an express written statement confirming that any violations have been fixed, no further action may be taken against the controller. However, after April 1, 2026, the attorney general will no longer have to give notice or wait to bring an enforcement action, and can pursue enforcement even if a violation was corrected.

J. Tennessee Information Protection Act ("TIPA")

The Tennessee Information Protection Act was signed into law on May 11, 2023, and will go into effect on July 1, 2025. TIPA applies to companies and businesses that do business in Tennessee or target products and services to Tennessee consumers, and:

- have more than $25 million in revenue;
- control or process personal information of at least 175,000 Tennessee consumers; or
- control or process information of at least 25,000 Tennessee consumers if the entity derives over 50% of gross revenue from sale of that data.

TIPA defines "personal information" broadly to include "information that identifies, relates to, or describes a particular consumer or is reasonable capable of being directly or indirectly associated or linked with, a particular consumer," so as to be applicable to any information relating to individual consumers. This includes personal identifiers, education, employment, financial information, medical information, biometric data, internet activity, as well as other personal information that can be used to create a profile of a consumer.

Consumer Rights

1. **Right to Confirm** whether a controller is processing personal data.

2. **Right to Access** their personal information.

3. **Right to Correct** any inaccuracies in their personal information, but limited to data the consumer previously provided.

4. **Right to Delete** personal data.

5. **Right to Request** a copy of their personal information held about them in a portable and usable form.

6. **Right to Opt-Out** of the sale of personal information, targeted advertising and profiling through automated means.

7. **Right to Appeal** any denial of a consumer request relating to the above rights.

Controller Obligations

Under TIPA, controllers must:

1. Limit the purpose of processing personal information to that which is reasonably necessary and proportional;

2. Take steps to implement reasonable safeguards for the personal information within their control;

3. Refrain from discriminating against consumers for exercising their rights and from processing personal information in violation of federal laws that prohibit discrimination;

4. Be transparent in their reasonably accessible, clear, and meaningful privacy notice; and

5. Ensure contracts control relationships with their processors.

Privacy Notice. Controllers are required upon a authenticated consumer request to provide a reasonably clear and meaningful privacy notice that includes the controller's purpose for

processing personal information and the categories of data that are being processed and/or sold to third parties, if any.

Enforcement. Tennessee's Attorney General is allowed under TIPA to investigate any individual who has engaged in a TIPA violation and bring about an appropriate declaratory, injunctive and monetary penalty, including a $7,500 civil penalty for each violation, in addition to attorney's fees and investigative costs. Entities found in violation of the law will be granted a 60-day cure period.

K. Texas Data and Privacy Security Act ("TDPSA" or "Texas Privacy Act")

On June 18, 2023, the Texas governor signed the Texas Data Privacy and Security Act which closely resembles the other 9 states' comprehensive privacy laws. The TDPSA will go into effect on March 1, 2024. The Texas Privacy Act applies to any entity that:

- conducts business in Texas or produces a product or service consumed by residents of the state;
- processes or sells any volume of personal data; and
- is not a small business, as defined by the U.S. Small Business Administration.

Unlike other states, the TDPSA applies more broadly, applying to both individuals and entities regardless of the number of individuals whose personal data is being processed, and regardless of revenue.

Consumer Rights

1. **Right to Confirm** whether a controller is processing personal data.
2. **Right to Access** their personal data and to obtain a portable copy of the personal data.
3. **Right to Correct** any inaccuracies in their personal data.
4. **Right to Opt-Out** of data processing for purposes of targeted advertising, the sale of personal data, and profiling (limited to "solely automated processing").
5. **Right to Delete** personal data provided by or obtained about the consumer.
6. **Right to Appeal** a controller's refusal to take action of a privacy rights request.

Similarly to other state privacy laws, controllers have 45 days to respond to consumer requests to exercise their rights under the TDPSA.

Controller Obligations

Under the TDPSA, controllers are required to:

1. Provide consumers with a privacy notice;

2. Limit the collection of personal data to what is relevant and reasonably necessary to the purpose of processing, as disclosed to the consumer;

3. Implement reasonable safeguards for the protection of personal information and conduct data protection assessments for high-risk processing activities;

4. Obtain consumer consent before processing sensitive personal information;

5. Refrain from discrimination against consumers for exercising their rights;

6. Enter into contracts with processors containing specific provisions; and

7. Clearly disclose the sale of any personal data to third parties or processing of data for targeted advertising.

Privacy Notice. In the privacy policy, a controller must disclose whether or not it will sell sensitive personal data or biometric data. If a controller sells sensitive consumer data, a privacy notice must include the language: "NOTICE: We may sell your sensitive personal data" or "NOTICE: We may sell your biometric personal data." The notice must also include the categories of personal data being processed, including sensitive data, the purposes of the processing, how consumers may exercise their rights, and the categories of data that are being shared with third parties.

Enforcement. The Texas Attorney General has sole enforcement rights on any TDPSA violation and must give 30 days' notice to any person or entity found in violation of the law. The person or entity then has 30 days to cure the violation. This right to cure is only applicable if the controller provides a written statement with supporting documentation that the violation has been cured. This right to cure does not sunset. The penalty for a TDPSA violation may include a $7,500 civil penalty per violation.

L. Oregon Consumer Privacy Act ("OCPA")

On July 18, 2023, the Oregon Consumer Privacy Act was signed, becoming the eleventh state to enact a consumer data privacy law. The OCPA will go into effect on July 1, 2024 (July 1, 2025 for non-profits). The OCPA applies to an individual who conducts business in Oregon or who provides products or services to Oregon residents and that during a calendar year:

- Controls or processes the personal data of 100,000 or more Oregon residents; or
- Controls or processes the personal data of 25,000 or more consumers while deriving 25% or more of the person's annual gross revenue from selling data.

Similarly to the CCPA, but unlike most other state privacy laws, the OCPA exempts only *data* governed by HIPAA and GLBA, rather than the *entities* subject to the two laws. It exempts certain financial institutions, such as banks and credit unions that only engage in financial activities.

Consumer Rights

1. **Right to Know** whether controllers are processing their data, as well as the categories of data being processed and third parties the data has been disclosed to.

2. **Right to Correction** of inaccuracies in their data.

3. **Right to Delete** their personal data held by a controller.

4. **Right to Opt-Out** of the processing of their personal data for targeted advertising, sale, or profiling of the consumer in a way that produces legal effects.

5. **Right to Data Portability:** Copies of a consumer's personal data must be provided in a portable and usable format.

These consumer rights are more expansive under the OCPA than in most other states. In particular, Oregon residents are able to request the third parties which the controller has disclosed personal data, and the controller may choose to respond to a consumer request by either providing names of the third parties to which it has disclosed the consumer's personal data or the names of the third parties to which it has disclosed *any* personal data. No other state requires controllers to disclose the names of the third parties, only the categories of third parties.

The OCPA also defines "sensitive data" broadly and includes information regarding racial or ethnic background, religious beliefs, mental or physical condition or diagnosis, and sexual orientation, as well as location data, children's data, and biometric data. The OCPA is also the only state to include transgender or non-binary status or crime victim status in its definition of "sensitive data."

Controller Obligations

Under the OCPA, controllers are required to:

1. Provide a privacy notice with certain specified content (see below);

2. Limit the processing of personal data to that which is reasonably relevant and necessary for the purposes of the processing;

3. Establish a secure and reliable means for consumers to exercise their privacy rights;

4. Obtain a consumer's consent to process sensitive data;

5. Enter contracts with processors; and

6. Conduct and document data protection assessments before engaging in processing activities that present a heightened risk of harm.

Privacy Notice. In a privacy notice, a controller must specify the exact purpose for which data is being collected and processed. The notice must identify the controller and any business name that the controller uses in the state of Oregon. Notices must be reasonably clear and include the categories of data that the controller processes, an outline of how the consumer may exercise their rights, categories or personal data shared with third parties, a description of all categories of third parties, and how each third party may process personal data.

Enforcement. The Oregon Attorney General has exclusive authority to enforce the OCPA. The OCPA has a specific statute of limitations for the attorney general, stating the attorney general "shall bring an action…within five years after the date of the last act of a controller that constituted the violation for which the [attorney general] seeks relief." The attorney general may levy civil penalties up to $7,500 per violation. Businesses are provided a 30-day period to cure the violation. However, this cure period will sunset on January 1, 2026.

M. Delaware Personal Data Privacy Acy ("DPDPA")

Delaware became the twelfth state to enact a consumer data privacy law when Gov. John Carney signed the DPDPA on September 11, 2023. The DPDPA most closely resembles Connecticut's and Virginia's data privacy laws, and it will go into effect on January 1, 2025. The DPDPA applies to businesses that do business in Delaware or target products or services to Delaware consumers, *and* either:

- Control of process personal data of 35,000 or more Delaware consumers (excluding data controlled or processed solely for the purpose of completing payment transaction), or

- Control or process personal data of 10,000 or more Delaware consumers and derive more than 20% of gross revenue from the sale of that data.

These thresholds are much lower than in other states' privacy laws, which means more companies will be subject to the DPDPA. The DPDPA does not apply to government entities or nonprofit organizations.

Consumer Rights

1. **Right to Confirm** whether a controller is processing the consumer's personal data and access such personal data (unless such confirmation or access would require the controller to reveal a trade secret).

2. **Right to Correct** inaccuracies in the consumer's personal data.

3. **Right to Delete** personal data provided by, or obtained about, the consumer.

4. **Right to Obtain** a copy of the consumer's personal data processed by the controller, in a portable and readily usable format, as well as the categories of third parties to which the controller has disclosed the consumer's personal data.

5. **Right to Opt-Out** of the processing of the personal data for the purposes of targeted advertising, the sale of personal data, and/or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Similarly to Oregon, the DPDA defines "sensitive data" broadly, including data revealing status as transgender or nonbinary. It includes the "traditional" categories, such as data pertaining to racial/ethnic origin and religious beliefs, and biometric data.

Controller Obligations

Under the DPDPA, controllers are required to:

1. Limit the collection of personal data to what is relevant and reasonably necessary in relation to the purposes for which the data is being processed, as disclosed to the consumer;

2. Obtain consumer consent for the process of personal data for purposes that are neither reasonably necessary to, or not compatible with, the disclosed purposes for which personal data is processed;

3. Establish reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at use;

4. Refrain from discriminating against consumers for exercising their rights and from processing personal data in violation of federal laws that prohibit discrimination;

5. Be transparent in their reasonably accessible, clear, and meaningful privacy notice;

6. Ensure contracts control relationships with their processors.

Enforcement. The Delaware Department of Justice has sole enforcement authority, and is required to provide companies with a 60 day notice and cure period before any enforcement actions. Violation fines can be up to $10,500 per violation. Individuals are unable to bring a claim for violations. This provision has a sunset date of December 31, 2025, after which the Delaware Department of Justice may choose to provide an opportunity to cure an alleged violation, but it is not required.

N. New Jersey Data Protection Act ("NJDPA")

New Jersey became the thirteenth state, and the first of 2024, to sign a consumer data privacy law. Like other states, the law aims to protect personal information of the state's residents, and ensure that businesses and companies have data protection measures in place to safeguard sensitive and personal data. With Governor Philip Murphy's signature on January 8, 2024, the law will be effective one year after the date of signature. The NJDPA regulates controllers conducting business in New Jersey based on these two criteria:

- Process personal data of at least 100,000 consumers (excluding data processed solely for payment transactions); or
- Process personal data of at least 25,000 consumers while deriving revenue or receiving discounts from data sales.

The law excludes nonprofits, government entities, and certain regulated entities. Unlike other state data privacy laws, NJDPA excludes business contact data or personal data associated with employees residing in New Jersey. Unlike most other state data privacy laws, the NJDPA does not impose any revenue thresholds.

Consumer Rights

1. **Right to Confirm** whether a controller is processing personal data and to access said data.

2. **Right to Correct** inaccuracies in the consumer's personal data.

3. **Right to Delete** personal data provided by, or obtained about, the consumer.

4. **Right to Obtain** a portable copy of personal data.

5. **Right to Opt-Out** of the processing of the personal data for the 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.

No later than 6 months after the NJDPA goes into effect, a controller that processes personal data for the purposes of targeted advertising or the sale of personal data must allow consumers "to exercise the right to opt-out of such processing through a user-selected universal opt-out mechanism."

Controller Obligations

Under the NJDPA, controllers are required to:

1. Limit the collection of personal data to what is relevant and reasonably necessary in relation to the purposes for which the data is being processed, as disclosed to the consumer;

2. Establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data and to secure it from unauthorized access;

3. Clearly disclose to consumers if they sell personal data to third parties or process personal data for targeted advertising or profiling, and provide a clear method for consumers to opt out;

4. Not process "sensitive data" without the consumer's express consent, or in the case of a known child, in accordance with the Children's Online Privacy Protection Act. Sensitive data is defined as personal data revealing racial or ethnic origin; religious beliefs; mental or physical health condition or treatment; sex life or sexual orientation; financial information, including account access details; citizenship or immigration status; transgender or non-binary status; genetic or biometric data that could identify an individual; data collected from a known child; and geolocation data.

5. Not process personal data for targeted advertising, sale or profiling without express consent, where the controller knows, or willfully disregards, that the consumer is at least 13 years old but younger than 17 years old;

6. Process data in a non-discriminatory manner as defined under state and federal law;

7. Provide a mechanism for a consumer to revoke consent to process personal data that is at least as easy as the mechanism for them to have given consent, and to cease processing the data within 15 days of revocation of consent; and

8. Conduct a data protection impact assessment on the processing of personal data that presents a heightened risk of harm to the consumer, including targeted advertising, processing sensitive data, selling personal data, or processing for profiling, if the profiling presents an unreasonably foreseeable risk of unfair or deceptive treatment or disparate impact on consumers, financial or physical injury to consumers, or an intrusion offensive to a reasonable consumer upon their "solitude of seclusion, or the private affairs, or concerns."

Privacy Notice. Within a privacy notice, organizations are to describe: the categories of personal data processed; the purpose of processing; the categories of third parties to which personal data is disclosed; the categories of personal data shared with third parties; how consumers may exercise their rights and appeal a data rights request decision; how the organization notifies consumers of material changes to the privacy notice; and organizations also must provide an email address or other online system that the consumer may use to contact the business.

Investigations and Enforcement. Violations to the NJDPA are enforceable by the New Jersey Attorney General and are considered unlawful practices under the New Jersey Consumer Fraud Act. During the first 18 months after the effective date, the Division of Consumer Affairs must issue and notice and grant a controller a 30-day cure period before any enforcement action can be taken. The Act does not extend this cure period beyond the first 18 months following the effective date.

O. New Hampshire Data Protection Act (SB 255)

On March 6, 2024, New Hampshire Governor Chris Sununu signed SB 255, making New Hampshire the fourteenth state to enact a comprehensive data privacy law. The law will go into effect on January 1, 2025. It applies to persons that conduct business in New Hampshire or that produce products or services that are targeted to its residents. The New Hampshire law's thresholds for applicability are typically lower than those of other states, applying to those who, during a one-year period:

- Controlled or processed the personal data of no less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
- Controlled or processed the personal data of no less than 10,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.

Consumer Rights

1. **Right to Verify** if a controller is processing their personal data.

2. **Right to Rectify** inaccuracies in the consumer's personal data.

3. **Right to Erase** personal data provided by, or obtained about, the consumer.

4. **Right to Receive** a portable and easily usable copy of personal data

5. **Right to Opt-Out** of data-processing for targeted advertising, personal data sales, or profiling that solely results in automated decisions with legal or similarly significant implications.

Controller Obligations

Under the SB 255, controllers are required to:

1. Limit the collection of data to only what is adequate, relevant, and reasonably necessary for the intended purpose;

2. Establish and maintain administrative security practices to protect the confidentiality of consumer personal data

3. Not process sensitive data without obtaining the consumer's consent or, if the data concerns a known child, process the data in accordance with COPPA;

4. Provide an easy means for consumers to revoke consent; and

5. Not process personal data for targeted advertising purposes without consumer consent.

The bill also requires controllers to conduct a data protection assessment for each action that may present a risk of harm to a consumer.

Enforcement. The Attorney General has authority to enforce violations under the law, with no provision for a private right of action, and the bill does not specify any fines or penalties for noncompliance. The bill also provides a 60-day cure period for compliance violations for one year after enactment. Beginning January 1, 2026, the Attorney General will have the discretionary power to provide a cure period.

Privacy Notice. Within a privacy notice, a controller must establish a reliable and secure means for consumers to submit a request to exercise their rights. The privacy notice must include the categories of personal data being processed, the purpose for processing the personal data, how consumers may exercise their rights, categories of personal data that the controller shares with third parties, the categories of third parties with which the controller shares personal data, and an active e-mail address or other online mechanism that the consumer may use to contact the controller.

P. Kentucky Consumer Data Protection Act ("Kentucky CDPA")

On April 4, 2024, Kentucky became the fifteenth state to adopt a comprehensive data privacy law. Governor Andy Beshear signed the Kentucky Consumer Data Protection Act ("Kentucky CDPA"), going into effect on January 1, 2026. The Kentucky CDPA applies to controllers who either conduct business in Kentucky or produce products or services targeted to Kentucky residents who, either:

- Control or process personal data of at least 100,000 Kentucky consumers; or
- Control or process personal data of 25,000 Kentucky consumers and derive over 50% of gross revenue from the sale of personal data.

Consumer Rights

1. **Right to Confirm** whether a controller is processing their personal data and access their data, unless providing confirmation and access would require the controller to reveal a trade secret;
2. **Right to Correct** inaccuracies in their personal data;
3. **Right to Delete** their personal data;
4. **Right to Obtain** a copy of the personal data previously provided to the controller in a readily useable format (i.e., data portability); and
5. **Right to Opt Out** of the processing of their personal data for the purposes of targeted advertising, the sale of their personal data, or profiling.

The Kentucky CDPA requires controllers to respond to a customer request or inquiry within 45 days, unless it is "reasonably necessary" to extend that time frame and the controller notifies the consumer of the extension.

Controller Obligations

Under the Kentucky CDPA, Controllers are obligated to:

1. Limit the collection of personal data to what is "adequate, relevant, and reasonably necessary" to the disclosed purpose with which the data is processed unless the controller obtains the consumer's consent;

2. Establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data and to secure it from authorized access;

3. Disclose to consumers if they sell personal data to third parties or process personal data for targeted advertising and provide a clear method for consumers to opt out.

4. Not process "sensitive data" without the consumer's express consent, or in the case of a known child, in accordance with COPPA;

5. Process data in a nondiscriminatory manner as defined under state and federal law;

6. Conduct a data protection impact assessment on the processing of personal data created or generated on or after June 1, 2026 that presents a heightened risk of harm to the consumer, including targeted advertising, processing sensitive data, selling personal data, or processing for profiling, if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment or disparate impact on consumers, financial or physical injury to consumer, or an intrusion offensive to a reasonable consumer upon their "solitude seclusion, or the private affairs, or concerns."

The Kentucky CDPA differs from some other state data privacy laws, like California and Connecticut, in that is does not require controllers to allow consumers to opt out of processing their personal data by using universal opt-out mechanisms.

Enforcement. The Kentucky Attorney General has exclusive enforcement authority to enforce violations under the Kentucky CDPA. The law provides business a 30-day cure period for alleged violations before an enforcement action may proceed. Unlike many other state, Kentucky's cure period does not sunset at any time after the law goes into effect. Violations of the Kentucky CDPA may incur civil penalties of up to $7,500 per violation.

Privacy Notice. The Kentucky CDPA requires controllers to provide consumers with a "reasonably accessible, clear, and meaningful" privacy notice that includes the categories of data it processes, the purpose for processing the data, the categories of third parties which it may disclose the personal data, and which categories of data it may disclose. The notice must also

provide consumers information on how they may securely and reliably exercise their rights and appeal a controller's decisions.

Q. Nebraska Data Privacy Act ("NEDPA")

On April 17, 2024, Nebraska joined the growing number of state to enact comprehensive data privacy legislation, and becoming the fourth state of 2024 to do so. Governor Jim Pillen approved the NEDPA, which provides data protection rights to Nebraska residents and requires applicable businesses to comply with the new data security requirements. This law will go into effect on January 1, 2025. The NEDPA uses the same applicability standard as Texas and applies to an organization that:

- Conducts business in Nebraska or produces a product or service consumed by Nebraska residents;
- Processes or engages in the sale of personal data; and
- Is not a "small business" as defined by the federal Small Business Act as it existed on January 1, 2024.

Consumer Rights

1. **Right to Confirm** whether a controller is processing their personal data and access their data;

2. **Right to Correct** inaccuracies in their personal data, taking into account the nature of the personal data and the purposes of the processing of their personal data;

3. **Right to Delete** their personal data provided by or obtained about the consumers;

4. **Right to Obtain** a copy of the personal data previously provided to the controller in a portable and readily usable format (to the extent technically feasible)(i.e. data portability); and

5. **Right to Opt Out** of the processing of their personal data for the purposes of targeted advertising, the sale of their personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

The Nebraska Data Privacy Act requires controllers to respond to a customer request or inquiry within 45 days, unless it is reasonably necessary to extend that time frame and the controller notifies the consumer of the extension.

Controller Obligations

Under the Nebraska Data Privacy Act, Controllers are obligated to:

1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the disclosed purposes with which the data is processed – unless the controller obtains the consumer's consent;

2. Establish, implement and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue to protect the confidentiality, integrity, and accessibility of personal data; clearly and conspicuously disclose to consumers if they sell personal data to third parties or process personal data for targeted advertising and provide a clear method for consumer to opt out. Notably, similar to the California Consumer Privacy Act and the Connecticut Data Privacy Act, sale is broadly defined as the exchange of personal data for monetary or other valuable consideration by the controller to a third party;

3. Not process "sensitive data" without the consumer's express consent, or in the case of a known child, in accordance with COPPA. Sensitive data is defined as personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizen or immigration status; genetic or biometric data that is processed for the purpose of uniquely identifying an individual; personal data collected from a known child; or precise geolocation;

4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;

5. Discriminate against a consumer for exercising any of the consumer rights contained in the act; and

6. Conduct and document a data protection assessment of: the processing of personal data for purposes of targeted advertising; the sale of personal data; the processing of personal data for profiling, if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment or unlawful disparate impact on consumers, financial, physical or reputational injury to consumers, or a physical or other intrusion offensive to a reasonable consumer upon their "solitude or seclusion, or the private affairs or concerns," or other substantial injury to any consumer; processing sensitive data; or the processing of personal data that presents a heightened risk of harm to the consumer.

Enforcement. Like most other states, Nebraska's Office of the Attorney General has exclusive authority to enforce violations. The attorney general must issue the controller or processor a notice of violation prior to initiating any action. A controller or processor will then have 30 days to cure the violation. A court may impose civil penalties of up to $7,500 for each violation.

Privacy Notice. Controllers are required to provide consumers an accessible and clear privacy notice that includes: the categories of personal data processed by the controller; its purpose for processing the personal data; information on how consumers may exercise their rights and appeal a controller's decisions; the categories of all third parties to which it shares the personal data and which categories it shares and a description of at least two methods through which the consumer may use to submit a request to exercise a consumer right.

R. Maryland Online Data Privacy Act (Senate Bill 541)

On May 9, 2024, Maryland Governor Wes Moore sign Senate Bill 541, the Maryland Online Data Privacy Act, into law. This makes Maryland the eighteenth state to enact comprehensive data privacy legislation. This law will go into effect on October 1, 2025. The Maryland Online Data Privacy Act placed obligations on entities that conduct business in Maryland or provide products or services targeted to residents of Maryland and, within the calendar year:

- Control or process personal data of at least 35,000 Maryland consumers; or
- Control or process personal data of 10,000 Maryland consumers and derive more than 20% gross revenue from the sale of personal data.

The 20% threshold gross revenue requirement is significantly lower than other US State Data Privacy Laws. Like many other states, however, the Maryland Online Data Privacy Act exempts several categories of entities, such as state and city government agencies, financial institutions, non-profit organizations, and national securities organizations. The Act also exempts certain types of information and data, including credit-reporting data, data that has de-identified, data processed or maintained for emergency contact purposes, and data covered by the Drivers' Privacy Protection Act.

Consumer Rights

1. **Right to Confirm** whether a controller processes their personal data and, if so, access their data;

2. **Right to Correct** inaccuracies in their personal data;

3. **Right to Delete** personal data provided by or obtained about the consumer, unless retention of the data is required by law;

4. **Right to Obtain** a copy of the personal data held by the controller in a readily usable format (i.e., data portability) that allows the consumer to easily transfer their data to another controller; consumers also have a right to obtain a list of the categories of third parties to which the controller has disclosed their data or to which the controller has disclosed data generally; and

5. **Right to Opt Out** of the processing of their personal data for the purposes of targeted advertising, the sale of their personal data, or profiling.

The Maryland Online Data Privacy also requires controllers who received a consumer request seeking to exercise any of these rights to respond to the consumer within 45 days, unless reasonably necessary to extend the time and the controller notifies the consumer of the extension.

Controller Obligations

Under the Maryland Online Data Privacy Act, Controllers are obligated to:

1. Limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain the specific product or service, unless the controller obtains the consumer's consent;

2. Establish, implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data and to secure it from unauthorized access;

3. Provide a mechanism for consumers to revoke consent to the processing of their personal data that is at least as easy as the mechanism for them to have given consent, and to cease processing the data as soon as possible, but not later than within 30 days of revocation of consent;

4. Disclose to consumers clearly if they sell personal data to third parties or process personal data for targeted advertising or profiling, and provide a clear method for consumers to opt out;

5. Process data in a non-discriminatory manner and not discriminate against a consumer for exercising a consumer right;

6. Conduct a data protection assessment on the processing of personal data. A data protection assessment conducted a compliance with another law of similar scope is sufficient to satisfy this requirement;

7. Allow consumers to opt out of the processing of their personal data y using a universal opt-out mechanism. Maryland permits the use of universal opt-out mechanisms (UOOMs) approved by other states, such as California, Connecticut, and New Jersey.

Enforcement. The Maryland Office of the Attorney General has exclusive enforcement authority to enforce violations. A controller or processor will have 60 days after receiving a violation notice to cure the violation. A court may impose penalties of up to $10,000 for each violation, and $25,000 per repeated violation. Like most other states, Maryland's Online Data Privacy Act does not provide for a private right to action.

S. Minnesota Consumer Data Privacy Act (MCDPA)

Minnesota Governor Tim Walz signed the Minnesota Consumer Data Privacy Act ("MCDPA") on May 24, 2024, making Minnesota the 18th to enact comprehensive consumer data privacy legislation. The law will go into effect on July 31, 2025. The MCDPA applies to any person or entity that conducts business in Minnesota or offers products or services that are targeted to Minnesota residents and, within the calendar year:

- Control or process personal data of at least 100,000 Minnesota consumers; or
- Control or process personal data of 25,000 Minnesota consumers and derives over 25% of gross revenue from the sale of personal data.

These conditions most similarly reflect the Connecticut and Virginia consumer data privacy law models. However, unlike most other states, the MCDPA does apply to technology providers under Minnesota's educational data laws, such as entities that provide technology to schools.

Consumer Rights

1. **Right to Confirm** whether or not the controller is processing the consumer's personal data and to access that data, if being processed;

2. **Right to Correct** personal data, taking into account the nature of the data and the purposes of the processing of that data;

3. **Right to Require the Controller to Delete** personal data concerning the consumer, unless required by law to retain the data;

4. **Right to Data Portability** when data processing is done through automated means;

5. **Right to Obtain** a list of specific third parties to which a company has disclosed the consumer's personal information;

6. **Right to Opt-Out** of the processing of their personal data for the purposes of targeted advertising, the sale of their personal data, or profiling, where profiling is being performed by automated means that produce legal or similarly significantly effects concerning a consumer; and

7. **Right to Appeal** rights requests that have not been fulfilled.

Controller Obligations

Under the Minnesota Consumer Data Privacy Act, Controllers are obligated to:

1. Limit the collection of personal data to what is reasonably necessary, relevant and reasonably necessary in relation to the purposes for which the data is processed and disclosed to the consumer;

2. Avoid processing personal data for secondary reasons (purposes that are neither reasonably necessary to nor compatible with the initial disclosed purposes) without the consumer's consent;

3. Establish, implement and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue;

4. Not collect, process, or share sensitive data except where strictly necessary to provide or maintain a specific consumer-requested product or service;

5. Not process personal data in violation of laws that prohibit unlawful discrimination against consumers, and refrain from discriminating against consumers that exercise their rights;

6. Provide consumers with a reasonably accessible, clear, and meaningful privacy notice.

7. Disclose to consumers clearly if they sell personal data to third parties or process personal data for targeted advertising or profiling, and provide a clear method for consumers to opt out;

8. Document and maintain a description of the policies and procedures developed to comply with the requirements of the MCDPA, and must include (1) the name and contact information for the individual with responsibility for the policies, and (2) a description of policies and procedures developed to implement different aspects of MCDPA including data minimization principles.

Enforcement. The Minnesota Office of the Attorney General has exclusive enforcement authority to enforce violations. Until January 31, 2026, controllers have a 30-day period to cure alleged violations before enforcement action can take place. A court may impose penalties of up to $7,500 for each violation.

Privacy Notice. Under the MCDPA, controllers are required to provide consumers with an online privacy notice that is "reasonably accessibly, clear, and meaningful" on its homepage. The privacy notice must also contain the categories of personal data the controller processes, the purposes for processing the data, an explanation of consumer's rights and how they can exercise those rights, and the categories of third parties it may disclose the personal data and the categories of data it discloses. The policy must also include an active email address or an online mechanism for the consumer to directly contact the controller. Finally, the controller is also required to inform consumers of any material changes to the privacy notice and provide an opportunity for the consumer to withdraw consent.

T. Rhode Island Data Transparency Act and Privacy Protection Act (the "Rhode Island Data Privacy Act")

The Rhode Island Data Transparency and Privacy Protection Act was signed into law on June 28, 2024, and it will go into effect on January 1, 2026. The Rhode Island Data Privacy Act imposes obligations on controllers who conduct business in Rhode Island or produce products or services targeted to residents of Rhode Island, and who:

- Control or process personal data of at least 35,000 Rhode Island customers, excluding instances where controllers are processing data "solely for the purpose of completing a financial transaction"; or

- Control or process personal data of 10,000 Rhode Island customers and derived more than 20% of gross revenue from the sale of personal data.

Consumer Rights

1. **Right to Confirm** whether a controller processes their personal data and access such data, unless a trade secret would be revealed;

2. **Right to Correct** inaccuracies in their personal data;

3. **Right to Obtain a Copy** of their personal data held by the controller in, where feasible, a "readily usable format" (i.e., data portability);

4. **Right to Delete** their personal data; and

5. **Right to Opt-Out** of the processing of their personal data for the purpose of targeted advertising, the sale of their personal data, or profiling.

Controller Obligations

Under the Rhode Island Data Privacy Act, Controllers are obligated to:

1. Establish and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data;

2. Not process "sensitive data" without the customer's express consent.

3. Process data in a non-discriminatory manner as defined under state and federal law;

4. Provide a mechanism for a customer to revoke consent to process personal data where consent was required and to cease processing the data within 15 days of revocation of consent;

5. Provide a privacy notice that identifies all categories of personal data it collects, identify all third parties the controller sells (or may sell) the customers' personally identifiable information, and provide an active email address or other mechanism for the customer to contact the controller; and

6. Conduct a data protection impact assessment on the processing of personal data that presents a heightened risk of harm to the customer, including targeted advertising, processing sensitive data, selling sensitive data.

Unlike some states, Rhode Island does not require controllers to allow customers to opt-out of processing their personal data by using a universal opt-out mechanism ("UOOM").

Enforcement. The Rhode Island Attorney General has exclusive enforcement authority. Violations to the Rhode Island Data Privacy Act will constitute violations of Title 6 of Rhode

Island's Commercial Law, under which each violation can incur civil penalties of up to $10,000. The Attorney General may bring an action for injunctive relief to curb identified violations.