

Iowa Becomes Sixth State to Pass Comprehensive Data Privacy Law

Becky Burr, Adrienne E. Fowler, and Daeyeong Kim

Iowa has joined California, Colorado, Connecticut, Utah, and Virginia as the sixth state to enact a comprehensive data privacy law. Iowa's House and Senate unanimously passed [Senate File 262](#), and Governor Kim Reynolds signed the bill on Tuesday, March 28, 2023. Iowa's Consumer Data Protection Act ("ICDPA" or "Act") will become effective on January 1, 2025. The Act shares similarities with its counterparts, but also contains several differences that will contribute to the patchwork nature of data privacy legislation in the United States. Below is our high-level overview of the ICDPA's key definitions, scope, consumer rights, duties of controllers and processors, and enforcement provisions.

Definitions.

Consumer. The ICDPA defines a consumer as a natural person who is an Iowa resident acting in an individual or household context. Similar to Colorado, Connecticut, Utah, and Virginia,¹ Iowa excludes from its definition a natural person acting in a commercial or employment context. Children are defined as natural persons under the age of 13.

Personal data. A consumer's personal data includes any information that is linked or reasonably linkable to an identified or identifiable natural person. It excludes de-identified or aggregate data as well as publicly available information.

Sensitive data. Sensitive personal data includes the following categories of information: racial or ethnic origin; religious beliefs; mental or physical health diagnosis; sexual orientation; citizenship or immigration status; genetic or biometric data; personal data of a known child; and precise geolocation data.

Sale of personal data. Similar to Virginia and Utah,² Iowa defines the sale of personal data as an exchange of personal data for monetary consideration by a controller to a third party. By contrast, California, Colorado, and Connecticut define sale as the exchange of personal data for monetary or other valuable consideration.³

Scope.

The ICDPA covers persons who conduct business in Iowa or produce products or services targeted to consumers who are Iowa residents and one of the following: (i) control or process personal data of at least 100,000 consumers who are Iowa residents; (ii) control or process personal data of at least 25,000 consumers who are Iowa residents and derive over 50% of gross revenue from the sale of personal data. Iowa's scope is equivalent to that of Virginia's Consumer Data Protection Act ("VCDPA").⁴

¹ Colo. Rev. Stat. Ann. § 6-1-1303(6); Conn. P.A. 22-15 § 1(7); S. 227 § 13-61-101(10)(b), 2022 Gen. Sess. (Utah 2022); Va. Code Ann. § 59.1-575. The California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA"), contained a temporary exemption for personal information collected by a business in an employment context, Cal. Civ. Code § 1798.145(m)(1)(A), but this exemption expired on January 1, 2023. Cal. Civ. Code § 1798.145(m)(4).

² Va. Code Ann. § 59.1-575; S. 227 § 13-61-101(31)(a), 2022 Gen. Sess. (Utah 2022).

³ Cal. Civ. Code § 1798.140(ad)(1); Colo. Rev. Stat. Ann. § 6-1-1303(23)(a); Conn. P.A. 22-15 § 1(26).

⁴ Va. Code Ann. § 59.1-576(A).

Exemptions. Iowa exempts the state and any political subdivisions of the state, non-profit organizations, institutions of higher-education, financial institutions and their affiliates subject to the Gramm-Leach-Bliley Act of 1999 (“GLBA”), 15 U.S.C. § 6801 *et seq.*, entities subject to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Pub. L. No. 104-191, 110 Stat. 1936, and the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”), 42 U.S.C. §§ 17921-17954.

It also exempts certain kinds of information including protected health information regulated under HIPAA, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, the Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721 *et seq.*, the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232 *et seq.*, the Farm Credit Act, 12 U.S.C. § 2001 *et seq.*, the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§ 6501-6506, and data processed in the employment context.

Consumer Rights.

Iowa consumers will have the right to (i) confirm whether a controller is processing personal data, (ii) access such personal data, (iii) delete personal data provided by the consumer, (iv) obtain a portable copy of personal data, and (v) opt out of the sale of personal data and targeted advertising. Similar to Utah, Iowa does not provide a right to correct any inaccurate personal data or to opt out of profiling.

Data Controller Duties.

Data security practices. Controllers are required to implement reasonable administrative, technical, and physical data security practices to protect personal data.

Notice and opt-out provisions. Controllers are prohibited from processing personal data for a non-exempt purpose unless they provide clear notice and an opportunity to opt out of such processing. The notice must include the following information: (i) categories of processed personal data; (ii) purpose of processing personal data; (iii) method of exercising privacy rights, including the right to opt out of the sale of personal data and targeted advertising; (iv) categories of personal data shared with third parties; and (v) categories of third parties that receive personal data.

Processing sensitive data of children. When processing sensitive data of a known child, controllers must process such data in accordance with COPPA.

Data protection assessment. Unlike California, Colorado, Connecticut, and Virginia,⁵ Iowa does not require covered entities to complete a data protection assessment.

Processor Duties.

Processor duties include assisting the controller with the controller’s obligations to respond to consumer rights requests, implementing of security requirements for processing personal data, and notifying any security breaches of the processor.

Data processing agreement. Controllers and processors are required to enter a contract that governs the processor’s data processing procedures. The contract must include instructions for processing

⁵ While the CCPA, as amended by the CPRA, currently does have a data protection assessment requirement, Cal. Civ. Code § 1798.185(15)(A) directs the California Privacy Protection Agency to issue regulations that will require such assessments for businesses whose processing of personal data presents a “significant risk”; Colo. Rev. Stat. Ann. § 6-1-1309; Conn. P.A. 22-15 § 8; Va. Code Ann. § 59.1-580.

personal data, the nature and scope of processing, the type of data subject to processing, the duration of processing, and the rights and duties of both parties. The contract must also establish the duty of confidentiality for personnel that process personal data and the obligation to delete or return all personal data to the controller upon request; furnish information to the controller demonstrating the processor's compliance with its obligations upon request; and engage any subcontractor or agent pursuant to a written contract that establishes data processing duties.

Enforcement.

The attorney general has exclusive authority to enforce the ICDPA. Prior to initiating any action, the attorney general must provide the controller or processor with ninety (90) days written notice. If, within the ninety (90) day period, the controller or processor cures the noticed violation and provides an express written statement that the alleged violations have been cured and no further violations shall occur, the attorney general cannot initiate an action against the controller or processor. This cure period is longer than that of all other states.⁶

Remedies. Injunction and civil penalties (up to \$75,000 for each violation).

Private right of action. Iowa does not create a private right of action.

Next Steps for Businesses.

Design your data protection program to address differing jurisdictional requirements. While existing state privacy laws often contain more stringent requirements than the ICDPA, covered businesses still need to be mindful of the slight variations in definitions, exemptions, and enforcement timelines. Understanding Iowa's requirements will be especially important for businesses taking a jurisdiction-specific approach. Businesses with a single compliance plan should also compare their current plan with any additional, but not necessarily more stringent, requirements imposed by Iowa.

* * * *

For more information on this alert or HWG's data privacy, security, and governance practice, please contact [Becky Burr](#), [Adrienne E. Fowler](#), [Daeyeong Kim](#), or the HWG lawyer with whom you regularly work.

This advisory is not intended to convey legal advice. It is circulated to our clients and others as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.

⁶ California, Utah, and Virginia provide 30 days. Cal. Civ. Code § 1798.199.50; S. 227 § 13-61-402(3)(b), 2022 Gen. Sess. (Utah 2022); Va. Code Ann. § 59.1-584(B). Colorado and Connecticut provide 60 days. Colo. Rev. Stat. Ann. § 6-1-1311(d); Conn. P.A. 22-15 §11(b).