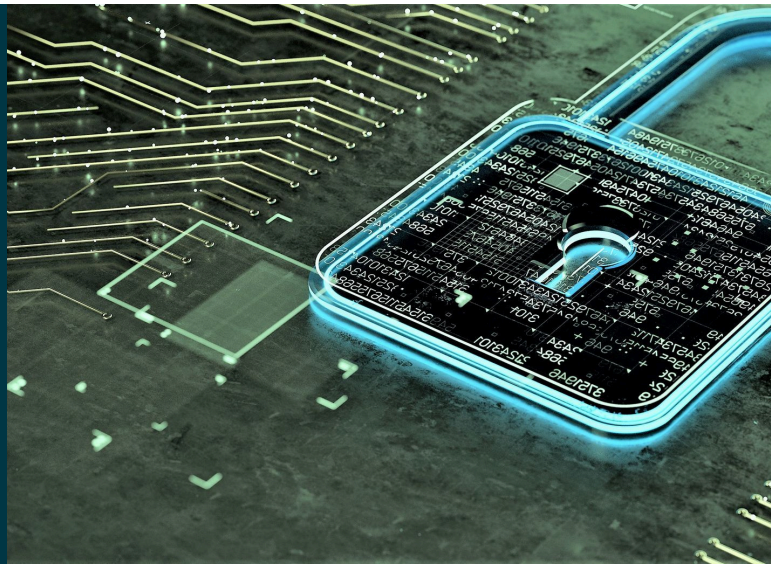
WILSON SONSINI



The Sixth State: Iowa Enacts Comprehensive Privacy Law

CONTRIBUTORS

Maneesha Mithal

Tracy Shapiro

Eddie Holman

ALERTS

April 4, 2023

On March 28, 2023, Iowa Governor Kim Reynolds signed "An Act Relating to Consumer Data Protection" (SF 262) (ICDPA),[1] making Iowa the sixth U.S. state to enact a comprehensive consumer privacy law following California, Virginia, Colorado, Utah, and Connecticut.

Substantively, the ICDPA is similar to Connecticut's recently enacted An Act Concerning Personal Privacy and Online Monitoring (CPOMA), the Utah Consumer Privacy Act (UCPA), the Colorado Privacy Act (ColoPA), and the Virginia Consumer Data Protection Act (VCDPA). The ICDPA will become effective on January 1, 2025.

Key Takeaways

- The ICDPA contains similar obligations and rights to existing U.S. state privacy laws in Virginia, Colorado, Utah, and Connecticut, but tracks most closely with the UCPA. Therefore, businesses already engaged in compliance efforts for those state laws will likely only have to implement minimal updates to comply with the ICDPA.
- The ICDPA does not include a right to correct personal data or opt out of profiling.
- The ICDPA's right to deletion only covers data provided *by* the consumer.
- The ICDPA's right to data portability is similar to the VCDPA in that the right is limited to consumer-provided data.
- The ICDPA is somewhat vague as to whether it provides consumers with a right to opt out of targeted advertising. On the one hand, it requires controllers that engage in targeted advertising to clearly disclose that activity and the manner in which a consumer may exercise the right to opt out. On the other hand, the section of the ICDPA that lists consumers' rights does not list a right to opt out of targeted advertising, just a right to opt out of the sale of personal data.
- The ICDPA requires notice and an opportunity to opt out of sensitive data processing, rather than an opt-in.
- The ICDPA's right to opt out of the sale of personal data does not include pseudonymous data, unlike the Connecticut, Colorado, Utah, and Virginia laws. The ICDPA also adopts the narrower definition of sale, which includes only an exchange for monetary consideration.
- The ICDPA does not include a private right of action; the ICDPA is exclusively enforced by the Iowa attorney general. The ICDPA is also subject to a 90-day cure period.

Scope

The ICDPA applies to persons (referred to as "controllers") that conduct business in Iowa or produce products or services targeted to Iowa residents (referred to as "consumers") and that during a calendar year: (1) controlled or processed the personal data[2] of at least 100,000 consumers or (2) controlled or processed the personal data of more than 25,000 consumers and derived more than 50

percent of gross revenue from the sale of personal data. The ICDPA's two threshold requirements are similar to other U.S. state privacy laws. Like the Virginia, Colorado, Utah, and Connecticut privacy laws, the ICDPA's definition of consumer excludes an individual acting in a commercial or employment context. The ICDPA includes broad, status-based, and data-based exemptions,[3] similar to previously enacted state laws such as the CPOMA and the VCDPA.

Consumer Rights

Compared to existing U.S. state privacy laws, the ICDPA grants consumers a more limited set of rights regarding their personal data. Specifically, the ICDPA grants consumers the right to (1) confirm whether a controller is processing their personal data and access that data; (2) delete personal data provided by the consumer; (3) data portability;[4] and (4) opt out of the sale[5] of personal data. The ICDPA does not include a right to correct, a right to not be subject to automated decision making, or the right to opt out of profiling. The ICDPA is vague as to whether it provides a right for consumers to opt out of targeted advertising, as it does not expressly list that right in the section of the act that lists other consumer rights, but it does require controllers to disclose whether they engage in targeted advertising and disclose the manner in which a consumer may opt out. Unlike the VCDPA, ColoPA, and CPOMA, the ICDPA does not require an opt-in choice for sensitive data[6] processing, but instead requires notice and an opportunity to opt out. Under the ICDPA, controllers have 90 days to respond to consumer requests, which is a longer time period than in other states. This time period can be extended once by an additional 45 days under certain circumstances.

Controller Obligations

The ICDPA imposes a number of duties on controllers, in keeping with other state privacy laws. Notable obligations include the following.

- Notice and opt-out before processing sensitive data (Section 715D.4(2)): Unlike the VCDPA and the ColoPA, which require opt-in consent prior to processing sensitive data, the ICDPA tracks closely with the UCPA, requiring notice and an opt-out instead. The ICDPA also delineates a new, explicit carve-out when defining certain categories as sensitive. Although racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, and citizenship or immigration status constitute sensitive data, there is an exception for data that is "used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law."[7] In other words, insofar as controllers use these types of personal data to comply with anti-discrimination laws, they would not need to offer an opt-out to consumers for the processing of that information.
- Privacy Policy (Section 715D.4(5)): The ICDPA also requires controllers to provide a privacy notice to consumers. Controllers that have already complied with privacy policy requirements for the CCPA and the VCDPA would be able to significantly leverage that work for ICDPA privacy policy compliance. Specifically, controllers must disclose the following to consumers under the ICDPA:
  - The categories of personal data (1) processed by the controller and (2) shared with third parties;
  - The categories of third parties with whom the controller shares personal data;
  - The purpose for processing personal data;
  - A description of a "secure and reliable" method for consumers to exercise their privacy rights under the ICDPA and appeal if necessary; and
  - If a controller sells or engages in targeted advertising, clearly and conspicuously state so and offer an opt out.

Other ICDPA controller obligations similar to other state privacy laws include (1) non-discrimination against consumers exercising privacy rights under the ICDPA and (2) adopting and implementing "reasonable, administrative, technical, and physical" data security practices.

Processor Obligations

Similar to the VCDPA, ColoPA, UCPA, and CPOMA, while the ICDPA defines "processor" as a person that processes personal data on behalf of a controller, determining who qualifies as a processor is a "fact-based determination" that depends upon the context in which personal data is to be processed.

Also similar to other states' privacy laws, the ICDPA requires processors to (1) adhere to controller instructions; (2) provide reasonable assistance to controllers to fulfill their obligations to respond to consumer rights requests; and (3) provide assistance to controllers to fulfill their data security and breach notification obligations. The ICDPA's contract requirements for controllers and processors are

also similar to other states' laws, such as CPOMA. Therefore, processors that have entered into a data processing agreement (DPA) that complies with the other five (California, Virginia, Colorado, Utah, and Connecticut) state laws can again significantly leverage that work for DPA compliance related to the ICDPA.

Enforcement and Civil Penalties

Like the Virginia, Colorado, Utah, and Connecticut laws, the ICDPA does not provide a private right of action. The Iowa attorney general has exclusive enforcement authority of the ICDPA. Before bringing an enforcement action, the attorney general must provide businesses with a written notice listing alleged violations; businesses then have 90 days to cure the violation, notify the attorney general, and provide a written statement confirming that no further violations will occur. If a controller or processor is still in violation after the cure period expires, or after sending a statement confirming that there will be no further violations, the attorney general may initiate civil proceedings. Violations of the law are subject to a $7,500 fine on a per violation basis.

Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy and data security issues and will monitor attorney general guidance, enforcement, and litigation pursuant to the ICDPA in order to assist clients with compliance. For more information or advice concerning your compliance efforts related to the ICDPA, please contact Tracy Shapiro, Maneesha Mithal, Eddie Holman, Nikhil Goyal, Yeji Kim, or any member of the firm's privacy and cybersecurity practice.

---

[1]Wilson Sonsini derived the ICDPA acronym from the Act's title: Iowa Consumer Data Protection Act.

[2]Consistent with laws passed in other states, the ICDPA defines personal data as "any information linked or reasonably linkable to an identified or identifiable natural person, excluding deidentified data, aggregate data – information relating to a group or category of consumers that excludes consumer identities and is not linked or linkable to any consumer – and publicly available information."

[3]The ICDPA extends status-based exemptions for state and local government entities, financial institutions, affiliates, and entities subject to the Gramm-Leach-Bliley Act (GLBA), covered entities and business associates subject to the Health Insurance Portability and Accountability Act (HIPAA) or the HITECH Act, nonprofit organizations, and institutions of higher education. The ICDPA extends certain data-based exemptions, particularly regarding protected health information under HIPAA and health records under related laws, regulations, and standards, and personal information regulated by the Children's Online Privacy Act (COPPA), the Fair Credit Reporting Act (FCRA), the Family Educational Rights and Privacy Act (FERPA), the Driver's Privacy Protection Act (DPPA), and the Farm Credit Act. Employment-related data are also exempt.

[4]The right to portability is limited to data provided by consumers.

[5]Consistent with the VCDPA's and the UCPA's narrow definition, the ICDPA defines "sale" of personal data as "the exchange of personal data for monetary or other valuable consideration by the controller to a third party." The right to opt out of a sale does not include pseudonymous data, unlike the Virginia, Colorado, Utah, and Connecticut laws.

[6]The ICDPA defines sensitive data to include the following categories of data: racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data that is processed for the purpose of uniquely identifying a natural person, personal data collected from a known child, and precise geolocation data.

[7]ICDPA § 715.1(26)(a).