

---

## Iowa Set to Become the Sixth State with a Comprehensive Privacy Law

MARCH 17, 2023

On Wednesday, March 15, the [Iowa House](#) passed [Senate File 262 \(SF 262\)](#), a comprehensive state privacy law similar to the ones that are already in effect in five US states. The bill had previously passed the Senate on March 6, and now moves to the Iowa Governor's desk for signature. If SF 262 is signed into law, Iowa would join California, Colorado, Virginia, Utah, and Connecticut as one of six states with a comprehensive privacy law in effect. Unlike the other states (all of which are in effect or set to go into effect in 2023), the Iowa bill would not go into effect until January 1, 2025.

Overall, this bill does not pose any substantive requirements for companies that do not already exist under the other five laws (from a comparison standpoint, the Iowa bill is closest to Utah's privacy law). It also has other business-friendly provisions, including a cure period, delayed effective date, and lack of a private right of action that will lessen the compliance burden faced by companies. Nonetheless, it is another reason for companies to review and revise their privacy compliance program and to assess whether they wish to provide certain privacy rights to all US consumers, especially states coalesce around Virginia and Utah as models.

In this post, we summarize key takeaways from the pending enactment of SF 262 and summarize the bill's key provisions. We are happy to answer any questions you might have about SF 262 and what it means for your company's privacy compliance programs.

### **KEY TAKEAWAYS**

- **An Industry-Friendly Bill:** Though companies will have to take the Iowa law into consideration when developing their compliance programs, the law does not create any new obligations for businesses that did not previously exist under the other laws. This will allow companies to expand their current compliance programs to account for Iowa, without needing to take any different compliance steps. The bill also has other business-friendly provisions. Most notably, the bill does not contain a private right of action, instead relying solely on the Iowa state attorney general (AG) for enforcement. In addition, controllers and processors can avail themselves of a 90-day cure period to resolve any deficient practices before the state AG may bring an enforcement action. Finally (and as we elaborate on

below), the law has broad exemptions for entities and data regulated under certain federal laws, limiting how “comprehensive” the law actually is.

- **Limited Enforcement Mechanisms:** In addition to the lack of a private right of action, SF 262 is also lacking various enforcement features prominent in other state privacy laws. For instance, the bill does not create any rulemaking authority for the state AG (unlike [Colorado’s law](#), for instance). Nor does the bill create a separate privacy-centered enforcement agency (like the [California Privacy Protection Agency](#)).
- **More Potential State Laws Incoming:** As our [state comprehensive privacy law updates](#) make clear, Iowa is unlikely to be the only state that passes a comprehensive state privacy law in 2023. As of this writing, bills in six other states — [Hawaii](#), [Montana](#), [Indiana](#), [New Jersey](#), [Oklahoma](#), and [Kentucky](#) — have passed a legislative chamber.
- **Potential Impact of Federal Legislation:** Looming over the passage of SF 262, of course, is the prospect of federal privacy legislation that could effectively override Iowa’s new law. [As we have previously written](#), Congress has made federal privacy legislation a priority this legislative session and appears poised to resurrect the American Data Privacy Protection Act (ADPPA), a bill considered last year that would have, among other things, [preempted](#) state comprehensive privacy laws like SF 262. The ADPPA remains far from enactment at the moment, but it remains possible that SF 262 could be preempted before it even takes effect.

## **KEY PROVISIONS**

Key provisions of SF 262 include the following:

- **Applicability Thresholds:** Applies to entities that conduct business in Iowa or produce products or services targeted to Iowa residents and do at least one of the following during a calendar year: (1) control or process personal data of at least 100,000 Iowa residents; or (2) control or process personal data of at least 25,000 Iowa residents and derive over 50% of gross revenue from sale of personal data.
- **Broad Exemptions:** Exempts various entities and information types, including state entities and political subdivisions of the state; financial institutions and data subject to GLBA; “certain organizations” governed by HIPAA (likely referring to both covered entities and business associates); nonprofit organizations; institutions of higher education; information governed by FCRA; personal data governed by FERPA; certain employment-related information; and personal data governed by COPPA.
- **Consumer Data Rights:** Creates rights for individual consumers, including: the right to confirm whether a controller is processing personal data and to access that data; the right to delete personal data; the right to obtain a portable and readily usable copy of personal data; and the right to opt out of the sale of personal data.
- **Privacy By Design:** Incorporates privacy by design principles, such as requiring data controllers to implement reasonable data security practices.
- **Sensitive Data Processing Requirements:** Requires that data controllers provide consumers with “clear notice and an opportunity to opt out” of the processing of sensitive data (which includes biometric information to the extent it is “processed for the purpose of

uniquely identifying a natural person”).

- **Privacy Notices:** Controllers must provide consumers with a privacy notice that identifies (1) categories of personal data processed; (2) purposes for said processing; (3) how consumers may exercise their consumer data rights; (4) categories of personal data the controller shares with third parties; and (5) categories of third parties with whom the controller shares personal data.
- **Disclosure of Data Sale and Targeted Advertising:** Controllers must “clearly and conspicuously disclose” the fact that they sell personal data to third parties or engage in targeted advertising, as well as the manner through which a consumer may opt out of such activity.
- **Processor Duties:** Imposes a range of requirements on processors, including, among other things, requiring that a contract govern a processor’s execution of data processing activities on behalf of the controller.
- **Enforcement:** Grants the state AG exclusive authority to enforce the Act. The state AG may seek injunctive relief and civil penalties of up to \$7,500 per violation.
- **Cure Period:** Prior to initiating an action, the state AG must provide a controller or processor with a 90-day cure period.
- **Effective Date:** The law would take effect on January 1, 2025.

---

## Authors



**Kirk J. Nahra**

**PARTNER**

Co-Chair, Artificial  
Intelligence Practice

Co-Chair, Cybersecurity  
and Privacy Practice

✉ [kirk.nahra@wilmerhale.com](mailto:kirk.nahra@wilmerhale.com)

☎ +1 202 663 6128



**Ali A. Jessani**

**COUNSEL**

✉ [ali.jessani@wilmerhale.com](mailto:ali.jessani@wilmerhale.com)

☎ +1 202 663 6105



**Genesis Ruano**

**ASSOCIATE**

✉ [genesis.ruano@wilmerhale.com](mailto:genesis.ruano@wilmerhale.com)

☎ +1 202 663 6154



**Samuel Kane**

**SENIOR ASSOCIATE**

✉ [samuel.kane@wilmerhale.com](mailto:samuel.kane@wilmerhale.com)

☎ +1 202 663 6114