Iowa Data Privacy Law Summary

On March 28, 2023, Governor Kim Reynolds (R) signed SF 262, the "Iowa Data Privacy Law" into law. The Act's provisions take effect on January 1, 2025. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Iowa Data Privacy Law** applies to a person conducting business in the state or producing products or services that are targeted to consumers who are residents of the state and that during a calendar year does either of the following: (a) controls or processes personal data of at least 100,000 consumers or (b) controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.
Covered Data	***"Personal data"***: any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" - does not include de-identified or aggregate data or publicly available information. ***"Sensitive data"***: personal data that includes: (a) racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, except to the extent such data is used in order to avoid discrimination on the basis of a protected class that would violate a federal or state anti-discrimination law; (b) genetic or biometric data that is processed for the purpose of uniquely identifying a natural person; (c) the personal data collected from a known child; (d) precise geolocation data.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. "Consent" may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action. Note that this only applies to the processing of sensitive data. ***"De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable natural person. ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. ***"Targeted Advertising"***: displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. ***"Sale of Personal Data"***: the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include: (a) the disclosure of personal data to a processor that processes the personal data on behalf of the controller; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer or a parent of a child; (c) the disclosure or transfer of personal data to an affiliate of the controller; (d) the disclosure of information that the consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience; (e) the disclosure or transfer of personal data when a consumer uses or directs a controller to intentionally disclose personal data or intentionally interact with one or more third parties; (f) the disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

Consumer Rights	• **Affirmative Consent:** A controller shall not process sensitive data concerning a consumer for a nonexempt purpose without the consumer having been presented with clear notice and an opportunity to opt out of such processing, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA. Note that this only applies to the processing of sensitive data. • **Access:** A consumer has the right to confirm whether a controller is processing the consumer's personal data and to access such personal data. • **Deletion**: A consumer has the right to delete personal data provided by the consumer. • **Portability:** A consumer has the right to obtain a copy of the consumer's personal data, except as to personal data that is defined as personal information pursuant to section 715C.1 that is subject to security breach protection, that the consumer previously provided to the controller in a portable and, to the extent technically practicable, 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. • **Opt Out Rights**: A consumer has the right to opt out of the sale of personal data.
Business Obligations	• **Responding to Consumer Requests**: A controller shall respond to a consumer without undue delay, but in all cases within90 days of receipt of a request. The response period may be extended once by 45 days when reasonably necessary,by informing the consumer of any such extension within the initial 90-day response period, together with the reason for the extension. A consumer has the right to a free response up to twice annually. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of any denied requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken in response to the appeal and provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint. • **Avoid Secondary Use**: A controller shall 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 unless the controller obtains the consumer's consent. • **Data Security**: A controller shall adopt and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue. • **No Unlawful Discrimination:** A controller shall not process personal data in violation of state and federal laws that prohibit unlawful discrimination against a consumer. A controller shall not discriminate against a consumer for exercising any consumer rights. • **Transparency**: A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes (1) the categories of personal data processed by the controller; (2) the purposes for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties; (5) the categories of third parties, if any, with whom the controller shares personal data. • **Disclosure**: A controller shall clearly and conspicuously disclose the sale of personal data to third parties or processing of personal data for targeted advertising in addition to the manner in which a consumer may exercise the right to opt out of such activity.

Controller / Processor Distinction	• **A processor shall assist the controller** in meeting its obligations under the Iowa Data Privacy Law. A contract between a controller and a processor shall govern the processor's data processing procedures and shall set forth instructions for processing personal 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 contract shall also include requirements that the processor shall: (1) ensure that each person processing personal data is subject to a duty of confidentiality; (2) delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) make available to the controller all information in its possession necessary to demonstrate the processor's compliance with obligations; (4) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor.
Exceptions and Exemptions	• A controller may disclose pseudonymous data or de-identified data with an exercise of reasonable oversight to monitor compliance with any contractual commitments. • The Iowa Privacy Law shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law-enforcement agencies; (d) prepare for and defend legal claims; (e) providing a product or service requested by a consumer; (f) protect interests essential for life or physical safety of the consumer; (g) prevent, detect and protect against security incidents; (h) preserve the security of systems; (i) investigate, report or prosecute those responsible for any such action; (j) engage in scientific or statistical research in the public interest; (i) assist third parties with the obligations of the Iowa Privacy Law. • Data exempt from the Iowa Privacy Law includes: protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, and COPPA.
Enforcement	• The Iowa Privacy Law does not provide the basis for, or be subject to, a private right of action to violations of this Act. • **Right to Cure**: The Attorney General shall have exclusive authority to enforce violations of the Act and shall provide a controller or processor 90 days' written notice identifying specific provisions being violated. Any controller or processor that violates the Act is subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation. All civil penalties collected under the Act shall be paid into the consumer education and litigation fund established under 714.16C. There is no sunset specified for the right to cure.