Blogs
April 12, 2021
Colorado Joins Ranks of States Introducing Consumer Data Privacy Legislation

On March 19, 2021, Colorado State Senators Richard Rodriguez (D) and Paul Lundeen (R) introduced Senate Bill 21-190 as part of a bipartisan effort to make Colorado the latest state to implement comprehensive legislation establishing certain consumer data privacy rights. Dubbed "A Bill for an Act Concerning Additional Protection of Data Relating to Personal Privacy," SB 21-190 largely follows in the footsteps of California's CCPA, Virginia's CDPA and the European Union's GDPR with a stated intent to "empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate." **Who's Affected**: SB 21-190 applies to legal entities that (a) conduct business or produce products or services that are intentionally targeted to Colorado residents and (b) either (i) control or process personal data of more than 100,000 consumers per calendar year or (ii) derive revenue or receive a discount on the price of goods or services from the sale of personal data and control or process the personal data of at least 25,000 consumers. **Scope of "Personal Data"**: SB 21-190 defines "personal data" as "information that is linked or reasonably linkable to an identified or identifiable individual," with the exceptions of (a) de-identified data and (b) publicly available information.

1. "de-identified data" means data that do not identify an individual with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.
2. "publicly available information" means information (i) lawfully made available from federal, state or local government records, (ii) a controller has a reasonable basis to believe the consumer has lawfully made available to the general public or to widely distributed media; and (iii) made available to the general public by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

Exemptions: SB 21-190 does not apply to certain categories of personal data already governed by various state and federal laws, such as HIPAA, the Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act, Driver's Privacy Protection Act of 1994, Children's Online Privacy Protection Act of 1998 (COPPA), Family Educational Rights and Privacy Act of 1974 (FERPA), in each case to the extent the activity related to the personal data is in compliance with such existing governing law(s). SB 21-190 also does not apply to data maintained for employment records purposes. If a business processes personal data pursuant to an exemption under SB 21-190, the business bears the burden of demonstrating that the processing qualifies for the exemption. **Consumer Rights**: Similar to preceding data privacy legislation, SB 21-190 establishes various consumer rights, including:

1. **Right to opt out** of the processing of personal data concerning the consumer;
2. **Right to access** the consumer's personal data and confirm whether a controller is processing personal data concerning the consumer;
3. **Right to correct** inaccurate personal data collected from the consumer;
4. **Right to delete** personal data concerning the consumer;
5. **Right to obtain** the consumer's personal data in a portable and readily usable format up to two times per calendar year.

Duties of Controllers: Similar to preceding data privacy legislation, SB 21-190 utilizes concepts of data "controllers" and data "processors," where a "controller" is the person or entity that determines the purposes and means of processing personal data and the "processor" is the person or entity that processes personal data on behalf of the controller. Controllers and processors must enter into a binding contract governing the processing instructions. Controllers do not avoid responsibility by delegating processing responsibilities to a processor. Under SB 21-190, controllers have certain duties to consumers, including:

1. **Duty of transparency**: The controller must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:
    1. The categories of personal data collected or processed by the controller or a processor;
    2. The purposes for which the categories of personal data are processed;
    3. An estimate of how long the controller may or will maintain the consumer's personal data;
    4. An explanation of how and where consumers may exercise their rights under SB 21-190;
    5. The categories of personal data that the controller shares with third parties, if any; and
    6. The categories of third parties, if any, with whom the controller shares personal data.

If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may object to the sale or processing. A controller may not require consumers to create a new account in order to exercise a right, or, based solely on the exercise of a right, increase the cost of or decrease the availability of a product or service.

1. **Duty of purpose specification**: A controller must specify the express purposes for which personal data is collected and processed.
2. **Duty of data minimization**: A controller's collection of personal data must be adequate, relevant, and limited to what is necessary in relation to the specified and express purposes for which the data are processed.
3. **Duty to avoid secondary use**: A controller may not process personal data for purposes that are not necessary to or compatible with the specified and express purposes for which the personal data are processed, unless the controller obtains the consumer's consent.
4. **Duty of care**: A controller must take reasonable measures to secure personal data during both storage and use from unauthorized acquisition.
5. **Duty regarding sensitive data**: A controller must not process sensitive data concerning a consumer without obtaining the consumer's consent or, in the case of processing of personal data concerning a known child or student, without obtaining consent from the child's or student's parent or lawful guardian. SB 21-190 defines "sensitive data" as (i) personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status, (ii) genetic or biometric data that may be processed for the purpose of uniquely identifying an individual, or (iii) personal data from a known child.
6. **Data protection assessments**: Before engaging in processing that presents a heightened risk of harm to a consumer, a controller must conduct and document a data protection assessment of each of its processing activities that involves personal data acquired on or after the effective date of SB 21-190. SB 21-190 defines "processing that presents a heightened risk of harm to a consumer" as including the following: (i) processing personal data for purposes of targeted advertising or profiling; (ii) selling personal data; and (iii) processing sensitive data.

Enforcement: SB 21-190 expressly states that it does not authorize a private right of action. Instead, if SB 21-190 were to become law as currently drafted, the Colorado Attorney General and District Attorneys would have exclusive enforcement authority by bringing an action in the name of the state or on behalf of persons residing in the state. Enforcement actions could be subject to civil penalties or injunctions. If passed, the authors of the SB 21-190 would intend for it to take effect on January 1, 2023. **Takeaways**: SB 21-190 generally follows in the footsteps of the CCPA, CDPA and GDPR, albeit with various nuanced differences. Businesses already taking measures to ensure compliance with the aforementioned data protection laws will likely find that such measures support compliance with SB 21-190. Nonetheless, SB 21-190 is not yet a finished product. Accordingly, businesses that qualify under the "Who's Affected" section above should stay apprised of any developments as early signs indicate this bill may have bipartisan support in the Colorado legislature.

Explore more in

Privacy & Security