personal data in specific cases; (7) to receive personal data in a machine-readable format and the ability to transmit ~~send~~ it to another controller, if technically feasible ("data portability"); and (8) to request that decisions based solely on automated processing concerning the consumer or significantly affecting the consumer and based on a consumer's personal data, are made by human beings or to challenge a decision.

For further clarification - the GDPR does not, necessarily, apply to a company simply because it collects data from citizens of the EU over the internet. Specifically, the company must actively market its products and services to those in the EU. It is a factual determination. For example, routinely shipping goods to the EU, utilizing the French language on the website (in addition to English) and setting a website up to accept euros would likely result in the GDPR applying to a given company.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In 2018, California became the first U.S. state to adopt a comprehensive privacy law, applicable beyond the insurance industry, imposing broad obligations on businesses to provide consumers with transparency and control of their personal data. The California Consumer Privacy Act (CCPA) became effective in 2020. Since it was adopted, it was amended by the California Privacy Rights Act (CPRA), which becomes effective January 1, 2023. Additionally, the California Attorney General promulgated implementing regulations in 2020.

Scope

The CCPA, as amended by the CPRA (California law) applies to companies doing business in California that collect or process consumers' personal information and meet one of the following thresholds: (1) has annual gross revenue in excess of $25,000,000 in the preceding calendar year; (2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Exemptions

The law does not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), and its implementing regulations. It also does not apply to protected health information that is governed by the privacy, security, and breach notification rules issued by the U.S. ~~Department of Health and Human Services (~~HHS~~)~~. Furthermore, this law contains an entity-level exemption for HIPAA-covered entities or business associates governed by the privacy, security, and breach notification rules issued by HHS.

Consumer Rights

California law provides consumers with the following rights subject to certain limitations: (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale or sharing of personal information; (7) to limit the use and disclosure of sensitive personal information aside from permissible enumerated purposes; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Business Obligations

The law imposes the following obligations on all covered businesses: (1) prohibits retaining a consumer's personal information for longer than reasonably necessary for the disclosed purpose; (2) requires implementing reasonable security procedures and practices; (3) requires notice of the following: collection of personal information, including sensitive personal information, retention of information, right to opt out of sale and sharing, and financial incentives; (4) prohibits using sensitive personal information outside of enumerated purposes when a consumer has requested not to use or disclose such data.

Enforcement

The CPRA amends the CCPA by placing administrative enforcement authority with the California Privacy Protection Agency, a new state agency created by the CPRA. Under the CPRA, the California Attorney General retains authority for seeking injunctions and civil penalties. Additionally, if personal information is breached, the consumer can pursue a private civil action against the company.

[1] And even when information is "deleted," the CCPA right to deletion allows the business to "maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes."

B. Colorado Privacy Act (CPA)

Scope

The Colorado Privacy Act (CPA) takes effect on July 1, 2023. Subject to certain limitations this law ~~It~~ applies to entities that conduct business in Colorado or produce or deliver commercial products or services intentionally targeted to residents of Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers in a year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers. The law defines "controllers" as those that "determine the purposes for and means of processing personal data" and defines "processors" as those that "process data on behalf of a controller."

Exemptions

The law contains data-based exemptions (rather than entity-level exemptions) for protected health information collected, processed, or stored by HIPAA-covered entities and their business associates, and information and documents created by a HIPAA-covered entity for purposes of complying with HIPAA and its implementing regulations. Additionally, the law contains an exemption for any personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), and implementing regulations, if such collection, processing, sale, or disclosure is in compliance with that law.

Consumer Rights

The CPA provides consumers with the following rights: (1) to opt out of targeted advertising, sale of personal data, and profiling; (2) to confirm whether a controller is processing the consumer's personal data and the right to access such data; (3) to correct inaccuracies in personal data; (4) to delete personal data; and (5) to obtain the personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity.

Business Obligations

The CPA imposes affirmative obligations on controllers, including the following: (1) provide consumers with an accessible, clear, and meaningful privacy notice; (2) specify the express purposes for which personal data are collected and processed; (3) collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes; (4) not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes, without obtaining consent from the consumer; (5) take reasonable measures to secure personal data; (6) not process personal data in violation of any law that prohibits unlawful discrimination; and (7) not process a consumer's sensitive data without first obtaining the consumer's consent. Additionally, controllers are required to enter into contracts