APM & CO

AMIT, POLLAK, MATALON

MAY 2022

New Comprehensive US State Privacy Laws

How to Prepare?

APM & CO. AMIT, POLLAK, MATALON - 18 Raoul Wallenberg St., Tel Aviv, 6971915, Israel

A P M
& C O
AMIT, POLLAK, MATALON

The privacy landscape in the United States is changing rapidly. In the absence of an encompassing federal privacy law, several states – California, Virginia, Colorado, Utah and, most recently, Connecticut –have enacted or begun to enact comprehensive, GDPR-inspired privacy laws.

These laws are primarily aimed at enhancing the data rights of resident consumers in their online activities by applying responsibilities to companies doing business in their jurisdiction.

The following statutes will become effective during 2023:

- The California Privacy Rights Act (**CPRA**), amending the effective California Consumer Privacy Act (**CCPA**), will enter into force by January 1st, 2023.
- The Virginia Consumer Data Protection Act (**VCDPA**) shall enter into force by January 1st, 2023.
- The Colorado Privacy Act (**ColoPA**) shall enter into force by July 1st, 2023.
- The Connecticut SB 6 ("Act Concerning Personal Data Privacy and Online Monitoring") (**CTPA**) shall enter into force by July 1st, 2023, subject to Governor signature
- The Utah Consumer Privacy Act (**UCPA**) shall enter into force by December 31st, 2023.

It is noteworthy that 21 other states are actively considering comprehensive privacy legislation in 2022.

The growing legislative patchwork increases the complexity for companies, including those not located in the United States.

Importantly, since violations of these new laws may result in an injunction and civil penalties, companies will now have to prepare to incorporate additional obligations. Note that these laws do not create a private right of action, with the exception of the CRPA that establishes such right for data-security breaches.

We have prepared these guidelines to assist you in complying and understanding the upcoming regulations.

Assess Whether the New Laws Apply to You

The CPRA, VCDPA, ColoPA, UCPA and CTPA may have ex-territorial jurisdiction, as they apply to companies that:

1. Conduct business in California, Virginia, Colorado, Utah or Connecticut (respectively) or market their goods and services to residents of said states; and
2. Either: (a) Control or process the personal data of at least 100,000 resident consumers per annum; or (b) Control or process the personal data of at least 25,000 resident consumers and derive more than 50% of their gross revenue from the sale of personal data (25% in Connecticut).

The UCPA and CRPA also apply a revenue threshold, applying only to business with annual revenue of $25 million or more.

The statutes exempt government entities, nonprofits, entities subject to the Health Insurance Portability and Accountability Act ("HIPAA"), higher education institutions, and financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA"). All statutes expressly exempt de-identified data and publicly available information.

Obtain Consents

Some of the statutes (VCDPA, ColoPA, CTPA) require affirmative consent (opt-in). Others, such as the UCPA and CPRA require only notification and offering an opt-out mechanism such as "do not sell" links.

Implement a broad Opt-Out Mechanism

All statutes require businesses to clearly disclose the sale of personal data and allow consumers to opt out of such sales. In addition, the new laws provide consumers with the right to opt out of targeted advertising as well as from profiling that may produce legal effects.

Implement an Appeals Process for a Denial of Data Subject Requests

The statutes provide consumers with certain data rights, including the right to access and delete their data (with certain limitations in some states). Consumers also have the right to data portability and the right to opt-out of certain uses of their data. Submitting a request or appealing a refusal to respect a request by a controller must be conspicuously available and easy to use. The appeal process is limited in time, generally, data subject requests should be responded to within 45 days.

Implement a data retention schedule

Businesses subject to the CCPA/CPRA will now be required to disclose the periods of time they intend to retain each category of personal data collected from a consumer. If this is not possible, the business can disclose the criteria it uses to establish that period.

Conduct Data Protection Impact Assessments for High Risk Data Processing

The VCDPA, ColoPA and CTPA require companies to conduct mandatory Data Protection Impact Assessments if they use personal data for sensitive or risky activities, for example: profiling, targeted advertising, selling or sharing consumers' personal data. Forthcoming regulations will introduce similar requirements in California. Note that under the ColoPA, the Data Protection Impact Assessment must be conducted before initiating the processing of data.

Conclusion

Companies should evaluate whether they will be subject to the new state privacy laws and take steps to understand their data flows, prepare processes to respond to data subject requests, and try to identify a common set of practices that will enable them to comply with these new obligations.

	California (CPRA amending the CCPA)	Virginia (VCDPA)	Colorado (ColoPA)	Utah (UCPA)	Connecticut (CTPA)
Effective	1.1.2023	1.1.2023	1.7.2023	31.12.2023	1.7.2023 (subject to Governor signature)
Private Right of Action	Only in the event of a data breach that compromises "personal information	No	No	No	No
Obligation to Notify Before or During Collection	Yes	Yes	Yes	Yes	Yes
Collection of Sensitive Personal Data	Opt-out	Opt-in	Opt-in	Opt-out	Opt-in
Right to Access	Yes	Yes	Yes	Yes	Yes
Right to Correct	Yes	Yes	Yes	No	Yes
Right to Delete	Limited to data obtained from the consumer	Yes	Yes	Limited to data obtained from the consumer	Yes
Opt-Out of Sales and Targeted Advertising	Including sharing of personal data	Yes	Yes	Yes	Yes
Opt-in for sales, targeted advertising and profiling of minors	Yes, to age 16	Yes, to age 13	Yes, to age 13	Yes, to age 13	Yes, to age 16
Opt-out of profiling	No	Yes	Yes	Silent	Yes
Non-Discrimination for Exercising Consumer Rights	Yes	Yes	Yes	Yes	Yes

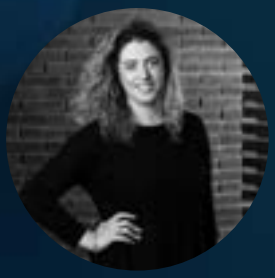
Timeline to Respond to Consumer Rights Requests	45 days	45 days	45 days	45 days	45 days
Right to appeal	No	Yes	Yes	No	Yes
Requirement to conduct Data Privacy impact Assessments for high-risk data processing	Pending regulations	Yes	Yes	No	Yes
Implement and Maintain Reasonable Administrative, Technical, and Physical Data Security Practices	Yes	Yes	Yes	Yes	Yes
Written Contracts with Processors	Required between Businesses and "Contractors"	Required between Businesses and Processors	Required between Businesses and Processors	Required between Businesses & Processors	Required between Businesses and Processors
Regulator	CPRA creates the California Privacy Protection Agency	Attorney General	Attorney General and District Attorneys	Attorney General	Attorney General
Civil Penalties	$2,500-$7,500	Up to $7,500 per violation	Up to $20,000 per violation	Actual damages to the consumer and up to $7,500 per violation in civil penalties	Up to $5,000 under CT Unfair Trade Practice Act
Opportunity to Cure	Eliminated	30-day	60-day	30-day	60-day

A P M
& C O
AMIT, POLLAK, MATALON

This document is intended to provide only a general background regarding this matter. This document should not be regarded as setting out binding legal advice, but rather a practical overview that is based on our understanding. APM & Co is not licensed to practice law outside of Israel.

Like the CPA, the VCDPA, and the CPRA (except for data-security breaches), the UCPA does not create a private right of action. Instead, the law authorizes the Consumer Protection Division of the Utah Department of Commerce to receive and investigate consumer complaints and alleged violations of the statute and refer violations to the Utah Attorney General. Upon referral, the Attorney General can sue to enforce the law but may only do so after providing an entity 30 days to cure alleged violations. If the violation persists, the Attorney General may seek damages of up to $7,500 per violation.

Contact



HILLA SHRIBMAN | Privacy and Data Protection
hillas@apm.law

ITAMAR BEN DAVID | Privacy and Data Protection
IItamarBD@apm.law