COMPARING COMPREHENSIVE US PRIVACY LAWS:

A GUIDE TO COMPLIANCE

UPDATED MAY 2023

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

OneTrust DataGuidance™ Regulatory Research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Contributors

OneTrust DataGuidance™: Angela Potter, Keshawna Campbell, Anna Bardin, Harry Chambers, Alice Muasher, Marcello Ferraresi, Bahar Toto, Francesco Saturnino Victoria Prescott

Image production credits
Cover photo: Liliboas / Signature collection / istockphoto.com

Published by OneTrust DataGuidance Limited, Dixon House, 1 Lloyd 's Avenue, London EC3N 3DS

Website **www.dataguidance.com**

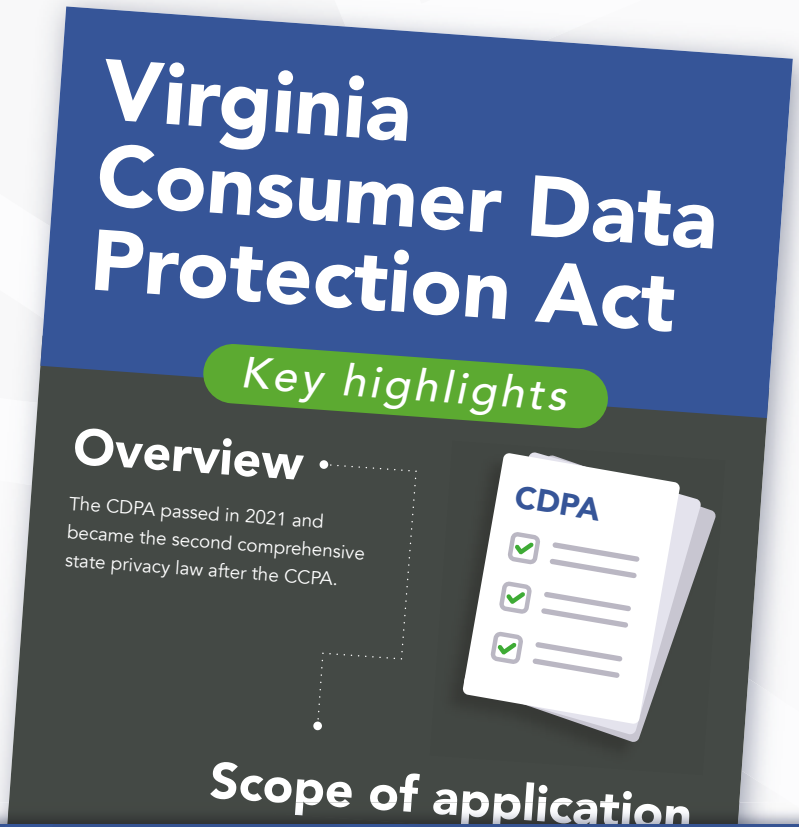
Table of contents

INFOGRAPHIC

Virginia CDPA Overview

Get to know the key components of the CDPA:
Definitions, timelines, scope of application, exemptions, enforcement, consumer rights, and more

Download Now



Introduction

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Following the entry into effect of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') on 25 May 2018, privacy became a much bigger focus for many companies around the world. The US was no exception, with California following suit soon after, with the California Consumer Privacy Act of 2018 ('CCPA') which entered into effect on 1 January 2020 with an enforceability date of 1 July 2020.

Notably, on 4 November 2020, the California Privacy Rights Act of 2020 ('CPRA') passed the 2020 California General Elections, and although it became effective immediately, most of its provisions became operational at a later date. The CCPA as amended by the CPRA (collectively 'the CCPA as amended') further strengthened the privacy requirements.

This wave brought other State attempts to adopt their own comprehensive privacy laws, with many failing to pass through the legislative session, but with some succeeding.

The first State to follow in California's footsteps was Virginia, after the Virginia Governor signed, on 2 March 2021, House Bill 2307 and its State Senate companion bill 1392 relating to the Consumer Data Protection Act ('CDPA'), with an entry into effect date of 1 January 2023. The CDPA does not contain provisions of similar strength to California's amended law, but is nevertheless a strong first step.

Three months later, Colorado's Governor signed, on 7 June 2021, Senate Bill 21-190 for an Act concerning additional protection of data relating to personal privacy, or the Colorado Privacy Act ('CPA'), with an entry into effect date of 1 July 2023. As with Virginia, Colorado's provisions are not as strong as those found in California's CCPA as amended, but they do outline a number of rights and obligations aimed at preserving privacy.

The momentum from 2021 carried over into 2022, with Utah passing a comprehensive privacy law. Specifically, on 24 March 2022 the Utah Governor signed Senate Bill 227 for the Consumer Privacy Act ('UCPA') into law, with an entry into effect date of 31 December 2023.

Two months later, Connecticut also unexpectedly saw the passage of a comprehensive privacy law, with the Connecticut Governor signing Senate Bill 6 for an Act Concerning Personal Data Privacy and Online Monitoring into law on 10 May 2022, with an entry into effect date of 1 July 2023.

Most recently, Iowa became the sixth US State to adopt a comprehensive privacy law which largely mirrors Utah's UCPA. Iowa's Act relating to consumer data protection ('ICDPA') was signed by the State Governor on 28 March 2023, with an entry into effect of 1 January 2025.

Importantly, at a federal level, on 3 June 2022, a bipartisan group of U.S. Senate and U.S. House of Representative leaders released a discussion draft for the American Data Privacy and Protection Act ('ADPPA') which, on 20 July 2022, was passed with amendments by the U.S. House Committee on Energy and Commerce. The ADPPA is significant as it marks the first comprehensive federal privacy bill to gain both bipartisan and bicameral support. If enacted, it would pre-empt the majority of state and local laws, invalidating any similar provisions therein.

Furthermore, sector-specific privacy and security laws like Family Educational Rights and Privacy Act ('FERPA'), Health Insurance Portability and Accountability Act ('HIPAA'), Gramm–Leach–Bliley Act ('GLBA'), and others, would continue to apply solely and exclusively with respect to data subject to the requirements of such regulations.

With the US now having six comprehensive State privacy laws under its belt, and a federal privacy bill working its way through Congress, this OneTrust DataGuidance Research report analyses all six laws, as well as the ADPPA, drawing on the similarities and differences in their provisions in a number of key areas. Specifically, the report addresses scopes of application, certain key definitions, various legal bases for the processing of personal data, controller and processor obligations, compliance with data subject rights, and enforcement.

Please note that supplementary regulations have been issued under California's CCPA as amended, and Colorado's CPA; however, they will not be covered in this report. The report will focus solely on the privacy laws and should be read in conjunction with any supplementary regulations and guidance.

1. Scope of application

While the laws of California, Colorado, Connecticut, Iowa, Utah, and Virginia all detail the scopes of personal, material, and territorial application, they differ in the degree to which they apply. For example, while all laws apply to the personal information of individuals within each State, they differ with respect to their application to businesses and the threshold to be met by definition for a business. California's laws provide for higher thresholds to be met with respect to annual revenues, the number of individuals' personal information processed, or the percentage of its annual revenue derived from the sale of such data as compared to the laws of Colorado, Connecticut, Iowa, Utah, and Virginia. Notably, the ADPPA uses different terminology and applies more broadly to personal information of US citizens processed by businesses. Nonetheless, the federal law distinguishes between businesses it considers to be 'large data holders' and those it considers as 'small data' holders on the basis of revenue and number of individuals' personal information processed, with different provisions applicable to each.

Territorially, the differences are smaller, where all laws apply to individuals who are residents of the State. However, California differs slightly with its CCPA as amended in also addressing the applicability in situations where individuals are outside the State of California, while the other laws are silent on this matter. In contrast, the ADPPA applies broadly to all residents of the US and pre-empts all other state privacy laws.

Materially, all of these six laws apply to personal information in some capacity, although the exact definitions of this differ. Additionally, all six laws generally do not apply to types of data otherwise regulated through other federal legislation, such as certain health or financial data. Where they differ is in the application to other types of data, such as pseudonymous data addressed by Colorado's CPA, household data as addressed by Connecticut's CTDPA, or deidentified data as addressed by California and the other State laws. Similarly, the ADPPA, which is still a draft law, defines personal information and the act of processing rather broadly, although with different terminology to state laws. The ADPPA differs from the CCPA as amended as it excludes de-identified data from its material scope, and from the state laws generally as it expands the carveout for employee data by adding additional data categories to its definition.

Please note that further information may be provided in supplementary regulations or guidance issued by regulatory bodies.

1.1. Personal

California

Under the CCPA as amended, natural persons or consumers are afforded protections, with obligations set on businesses and how they process consumers' personal information. As such, the CCPA as amended notes that its provisions apply to personal information which is collected by a business from consumers.

In this respect, a 'consumer' is defined as a natural person who is a California resident, however they may be identified as well through any unique identifier.

Meanwhile, and broadly speaking, a 'business' is defined as a for profit entity that collects consumers' personal information and determines the purpose and means of the processing of this personal information, and which does business in California.

Additionally, a business must, in addition to the aforementioned requirement, meet one of the following thresholds:

- has an annual gross revenue in excess of $25 million;
- alone or in combination, annually buys, receives for its commercial purposes, sells, or shares for commercial purposes the personal information of 100,000 or more consumers or households; and
- derives 50% or more of its annual revenues from selling consumers' personal information.

Colorado

Similarly, the CPA applies to controllers and protects consumers and individuals who are residents of Colorado. More specifically, the CPA applies to controllers that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to residents of the State. In addition to this, such businesses must also satisfy at least one of two outlined additional requirements, namely that the business either controls or processes the personal data of 100,000 consumers or more during a calendar year, or which 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 consumers or more.

However, unlike California's CCPA as amended which details its personal scope of application through applied definitions, Colorado's CPA also expressly provides controllers to which its provisions would not apply, namely air carriers or certain national securities associations, which its general provision on scope of application.

Connecticut

Connecticut's CTDPA applies to persons that conduct business in Connecticut or persons that produce products or services that are targeted to residents of Connecticut. In addition to this requirement, such persons are also required to meet two further requirements, namely that during the preceding calendar year, they either controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or they controlled or processed the personal data of not less than 25,000 consumers and derived more than 25% of their gross revenue from the sale of such personal data.

In comparison the California's CCPA as amended and Colorado's CPA, the CTDPA also provides an extensive list of bodies to which it does not apply, namely:

- a body, authority, board, bureau, commission, district, or agency of Connecticut or of any political subdivision of Connecticut;
- non-profit organisations;
- institutions of higher education;
- certain national securities associations;
- certain financial institutions regulated by federal law; or
- covered entities or business associates as regulated by federal law.

Iowa

Similar to Utah's UCPA, the applicability of Iowa's ICDPA is dependent on covered entities meeting certain thresholds. In particular, the ICDPA applies to a person conducting business in Iowa or producing products or services that are targeted to consumers who are Iowa residents, and that, during a calendar year, does either of the following:

- controls or processes personal data of at least 100,000 consumers; or
- controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.

The ICDPA compares to the CDPA, CPA, CTDPA, and UCPA in clarifying what is not included within its personal scope of application, by outlining that the State or any of its political subdivisions, financial institutions, affiliates of financial institutions, or data subject to the GLBA, and persons subject to HIPAA are not subject to the ICDPA. In addition, non-profit organisations and/or institutions of higher education are not subject to the ICDPA.

Utah

Utah's UCPA applies to consumers and to both controllers and processors, although applicability is dependent on such controllers or processors meeting certain additional requirements. More specifically, they must be conducting business in Utah or producing products or services targeted towards consumers who are residents of Utah, have an annual revenue of $25 million or more, and satisfy one or more of the noted two additional requirements. Namely, and in addition to the aforementioned, such controllers or processors must also control or processes the personal data of 100,000 or more consumers in a single calendar year, or they must derive over 50% of their gross revenue from the sale of personal data and control or process such data of 25,000 or more consumers.

However, and similarly to Connecticut's CTDPA which extensively provides a list outside of this personal scope of application, the UCPA details that it does not apply to governmental entities or a third parties under contract with a governmental entity when acting on behalf of the governmental entity, and does not apply to tribes, institutions of higher education, non-profit corporations, or covered entities and business associates as regulated by applicable federal laws.

Virginia

Slightly differently to California's CCPA as amended, but quite similar to the laws of Colorado, Connecticut, and Utah, Virginia's CDPA applies to residents of Virginia, and to businesses. Specifically, it applies to those businesses which produce products or services targeted towards Virginia residents and that either control or process personal data of at least 100,000 consumers in a single calendar year, or that control or process personal data of at least 25,000 consumers and derive over 50% of gross revenues from the sale of such personal data.

The CDPA also compares to the CPA, CTDPA, and UCPA in detailing what is outside of its personal scope of application, namely any body, authority, board, bureau, commission, district, or agency of Virginia or of any political subdivision of Virginia, as well as any financial institution, covered entity, or business associate regulated by federal laws, and any non-profit organisation or institution of higher education.

USA Federal

Unlike the above-mentioned state laws, the ADPPA differs in some of its terminology and refers to a business/controller and data, namely as a 'covered entity' and 'covered data'. In this regard, the ADPPA stipulates that it applies to the processing of covered data relating to individuals and places obligations on covered entities.

In this respect, a 'covered entity' refers to any entity or person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring data and falls within the following categories:

- is subject to the Federal Trade Commission Act of 1914;
- is a common carrier subject to the Communications Act of 1934 as well as all acts amendatory thereof and supplementary thereto; or
- is an organization not organized to carry on business for its own profit or that of its members (including any entity or person that controls, is controlled by, or is under common control with the covered entity).

Furthermore, the ADPPA notes that the term 'covered entity' excludes public entities and any person or entity that processes personal data on behalf of a government entity insofar as it is acting as a service provider to the government entity.

Notably, the term 'individual' is defined as a natural person residing in the United States.

The ADPPA also refers to and places obligations on 'service providers' alongside covered entities. In this respect, a 'service provider' refers to a person or entity that processes covered data on behalf of a covered entity or a government entity and receives covered data from or on behalf of a covered entity or government entity.

1.2. Material

California
The CCPA as amended generally covers the processing of consumer personal information with processing defined as any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means. Furthermore, the CCPA as amended details obligations for the selling or sharing of personal information, and outlines specific circumstances in which such activities will not be considered sharing or selling. Moreover, the CCPA as amended does not apply to activities governed by other federal laws or State laws specific to certain sectors and fields.

Notably, and in contrast to the laws of the other States which are silent on this matter, the CCPA as amended is not limited to information collected electronically or over the internet but applies to the collection and sale of all personal information collected by a business from consumers generally.

Colorado
Colorado's CPA applies to personal data which is defined as information that is linked or reasonably linkable to an identified or identifiable individual, but not to certain personal data governed by listed state and federal laws such as certain protected health information, certain healthcare information, among others, and listed activities, and employment records.

One difference that the CPA provides is an express call out for data subject rights, noting that they do not apply to pseudonymous data if the controller can demonstrate that the information necessary to identify the consumer is kept separately and is subject to effective technical and organisational controls that prevent the controller from accessing the information.

Connecticut
In line with other State laws, the CTDPA applies to the personal data of individuals, which is defined as any information that is linked or reasonably linkable to an identified individual or an identifiable individual and excludes de-identified data or publicly available.

It does not, however, apply to other types of data regulated by federal laws, nor to data processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party when collected in the context of the role, as an emergency contact, or if otherwise necessary in certain circumstances.

Iowa
Similar to other State laws, the ICDPA applies to the 'personal data' of 'consumers' in general, which is defined as any information that is linked or reasonably linkable to an identified or identifiable natural

person, excluding de-identified, aggregate data or publicly available information, and persons who are Iowa residents and acting only in an individual or household context, excluding a natural person acting in a commercial or employment context.

Like the UCPA, the ICDPA outlines what is outside of its material scope of application, including, among other things, protected health information under HIPAA; data processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party to the extent that the data is collected and used within the context of that role; and personal data used in accordance with the federal COPPA, its rules, regulations, and exceptions.

Utah

Like the other State laws, the UCPA also applies to individuals' personal data, defined as information linked or reasonably linkable to an identified individual or an identifiable individual.

The UCPA also similarly outlines what is outside of its material scope of application, including, among other things, protected health information, patient identifying information, identifiable private information, deidentified information, or identifiable private information or personal data collected as part of human subjects research pursuant to federal and international laws and requirements.

Virginia

Finally, and no differently to the other State laws, the CDPA also places personal data of individuals within its material scope of application, defining this as information linked or reasonably linkable

to an identified or identifiable natural person, but does not include deidentified data or publicly available information. Although it slightly expands the definition to include the mention of deidentified and publicly available information, the wording is largely the same as the other laws. It too excludes data regulated by federal laws, calling out certain health and financial data.

USA Federal

Similar to state laws, the ADPPA material scope includes the processing of personal data relating to individuals, adopting the term 'covered data' throughout. In this respect, the ADPPA defines 'covered data' rather widely in comparison to state laws as information that identifies or is linked, alone or in combination with other information, to an individual or a device that identifies or is linked to an individual, and may include derived data and unique identifiers. Additionally, covered data excludes:

- de-identified data;
- employee data;
- publicly available information; or
- inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

Similarly, the ADPPA adopts a broad definition of processing, such that to process means to conduct or direct any operation or set of operations performed on covered data, including analysing, organising, structuring, retaining, storing, using, or otherwise handling covered data.

1.3. Territorial

California

The CCPA as amended presents the strongest direct address of the territorial scope of the law, as compared to those of Colorado, Connecticut, Iowa, Utah, and Virginia. Specifically, while noting

that it applies to California residents through its definition of 'consumer', to which it applies, it also addressed extraterritorial application in certain circumstances.

In addition, while the CCPA as amended details that its obligations on businesses do not restrict their ability to collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California, it also permits them to store personal information when the consumer is located in California, to then later collect and store that personal information when the consumer is outside of California.

Colorado

Unlike the CCPA as amended, the CPA is much more silent on its territorial scope of application, noting only that its provisions apply to businesses that conduct business or produce or deliver commercial products or services that are intentionally targeted to Colorado residents.

Connecticut

The CTDPA takes the same approach as Colorado, Utah, and Virginia with respect to its territorial application, noting also that it applies to controllers or processors conducting business in Connecticut or producing a product or service targeted toward Connecticut residents.

Iowa

The ICDPA takes the same approach as Colorado, Connecticut, Utah, and Virginia with respect to its territorial application, as it applies to controllers or processors conducting business in Iowa or producing products or services that are targeted to consumers who are Iowa residents.

Utah

Like Colorado, Connecticut, and Virginia, Utah's CPA also applies to controllers or processors conducting business in Utah, or producing a product or service targeted toward Utah residents.

Virginia

Finally, Virginia mirrors Colorado, Connecticut, and Utah in also providing that the CDPA applies to persons conducting business Virginia or producing products or services targeted to Virginia residents.

USA Federal

In contrast to state laws, the ADPPA applies to US residents as depicted from its definition of 'individual', to which it applies. Additionally, as a federal law, the ADPPA pre-empts state laws except for those listed in the ADPPA, which include consumer protection laws of general applicability and provisions of laws that govern privacy rights of employees and students.

Furthermore, the ADPPA, in its definition of a 'covered entity' seems to extend its applicability to include subsidiaries of US businesses.

Notably, in relation to enforcement, the ADPPA gives the California Privacy Protection Agency ('CPPA') the power to enforce the provisions of the ADPPA in the same manner it would otherwise enforce the CCPA as amended.

2. Definitions

There are several differences between the definitions in the comprehensive privacy laws of California, Colorado, Connecticut, Iowa, Utah, and Virginia. The main distinguishing factor is that California's CCPA as amended contains much more detailed definitions as compared to the comprehensive privacy laws of the other state laws. A good example is the definition of 'personal information' vs 'personal data'.

One other notable difference between the definitions of 'sensitive data' or 'sensitive personal information' is the very slight distinction in wording across the six laws, thereby potentially broadening or narrowing scopes of applicability.

On the definition of 'data subject', the six laws follow an identical approach in instead referring to 'consumers'. However, here too there is some deviation in definitions. California contains a broader definition, while the other five laws expressly note that a 'consumer' is acting in a household capacity and excludes any commercial or employment context.

Contrastingly, while California takes a similar approach for the definition of 'data controller' by instead defining 'business', the other five laws expressly define 'controller' taking a similar approach to the EU's GDPR. The same holds true for the definition of 'data processor', where instead of providing a detailed definition, Colorado, Connecticut, Iowa, Utah, and Virginia define it as the body acting on behalf of the controller. Here California also takes a different approach both in terminology and definition.

In even greater contrast, the proposed ADPPA does not utilise any of the aforementioned terminologies. Overall, the ADPPA provides extensive details within its definitions and elaborates precise exceptions for many of the key concepts. However, it favours 'covered entities', in line with other federal laws such as HIPAA. Further, there is no definition for 'consumer' or 'data subject', although the former is used within the text, but instead 'individual' or 'employee' are explicitly defined.

As with Californian legislation, the ADPPA also includes government identifiers, union membership information, and financial account numbers. However, the ADPPA goes beyond current state law protections by including login credentials and security codes within its definition of 'sensitive data'.

In addition, the ADPPA, if enacted, would also depart from the aforementioned state laws with regards to its treatment of children, which is defines as anyone under the age of 17 as opposed to either 13 or 16 in the state laws. Furthermore, the ADPPA prohibits targeted advertising to anyone 'known' to be a child, as well as the transfer of children's data without parental consent.

As such, the following section outlines key definitions of personal information, sensitive personal information, data subject, data controller, and data processor as these terms are defined under each of the six comprehensive state privacy laws, as well as the ADPPA.

Please note that further information may be provided in supplementary regulations or guidance issued by regulatory bodies.

2.1. Personal information

California

Under the CCPA as amended, 'personal information' means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. This category includes, but is not limited to, the following information:

- identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- any personal information that identifies, relates to, describes, or is capable of being associated with a particular individual, such as social security number, physical characteristics or descriptions, address, telephone numbers, or medical information, among others;
- characteristics of protected classifications such as, race, colour, religion, sex/gender, among;
- certain commercial information;
- biometric information;
- other electronic network activity information, such as browsing history;
- geolocation data;
- audio, electronic, visual, thermal, olfactory, or similar information;
- professional or employment-related information;
- education information;
- inferences drawn from any of the aforementioned information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes; and
- sensitive personal information.

This concept of 'personal information' does not include information that is publicly available, and also excludes information that is deidentified or aggregated.

Colorado

Contrastingly, Colorado's CPA contains a much shorter definition, and refers to 'personal data' rather than 'personal information', but bears some similarities. It provides that 'personal data' consists of information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information. In this context, publicly available information means any information that is lawfully made available, and information that a controller has a reasonable basis to believe is lawfully made available to the general public.

Connecticut

Like Colorado's CPA, Connecticut's CTDPA also refers to 'personal data', which includes any information that is linked or reasonably linkable to an identified or identifiable individual. De-identified data and publicly available information do not constitute 'personal data' under the CTDPA.

Iowa

Equally, under the ICDPA, 'personal data' means any information that is linked or reasonably linkable to an identified or identifiable natural person. De-identified or aggregate data or publicly available information are excluded from the concept of 'personal data'.

Utah

Similarly, under the UCPA 'personal data' means information that is linked or reasonably linkable to an identified or identifiable individual, with the exclusion of deidentified/aggregated data or publicly available information.

Virginia

Likewise, according to Virginia's CDPA, any information that is linked or reasonably linkable to an identified or identifiable natural person, excluding de-identified data or publicly available information, constitutes 'personal data'.

USA Federal

Under the ADPPA, 'covered data' means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers. The following types of data are excluded from the definition of covered data:

- de-identified data;
- employee data;
- publicly available information; or
- inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

In addition, the ADPPA defines 'employee data' in depth.

2.2. Sensitive personal information

California

Under the CCPA as amended, 'sensitive personal information' is defined as:

- personal information that reveals a consumer's:
  - social security, driver's license, state identification card, or passport number;
  - a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
  - precise geolocation;
  - racial or ethnic origin, religious or philosophical beliefs, or union membership;
  - the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; and
  - genetic data;
- the processing of biometric information for the purpose of uniquely identifying a consumer;
- personal information collected and analysed concerning a consumer's health; and
- personal information collected and analysed concerning a consumer's sex life or sexual orientation.

Sensitive personal information that is 'publicly available' is not considered 'sensitive personal information' nor 'personal information'.

Colorado

Colorado's CPA expressly defines 'sensitive data' providing that it is comprised of personal data revealing certain information (for example racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status), genetic or biometric data that may be processed for the purpose of uniquely identifying an individual, or personal data from a known child.

Connecticut

The CTDPA qualifies 'sensitive data' as personal data which includes:

- data revealing racial or ethnic origin;
- religious beliefs;
- sexual orientation, citizenship, or immigration status;
- mental or physical health condition or diagnosis information;
- the processing of genetic personal or biometric data, if the processing is for the purpose of identifying a specific individual;
- personal data collected from a known child; or
- precise geolocation data.

Iowa

The ICDPA mostly replicates the definition of 'sensitive data' under the CDPA. Specifically, 'sensitive data' under the ICDPA means a category of personal data that includes the following:

- 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;
- genetic or biometric data that is processed for the purpose of uniquely identifying a natural person;
- personal data collected from a known child; and
- precise geolocation data.

Utah

Similarly to Colorado and Connecticut, Utah's UCPA defines 'sensitive data' as:

- personal data revealing:
  - racial or ethnic origin, unless the personal data is processed by a video communication service;
  - religious beliefs;
  - sexual orientation;
  - citizenship or immigration status; or
  - medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional;
- the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or
- specific geolocation data.

However, and unlike the laws of Colorado, Connecticut, and Virginia, Utah also outlines what does not qualify within this definition. Specifically, data is not considered sensitive if processed by a person licensed to provide health care under applicable laws with respect to information regarding medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional. The only other state calling out an exception is California's CCPA as amended, in providing that publicly available data is not sensitive.

Virginia

The CDPA also takes a slightly limited approach in defining 'sensitive data', noting that it is a category of data that includes:

- racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
- the processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- the personal data collected from a known child; or
- precise geolocation data.

USA Federal

The ADPPA defines 'sensitive covered data' as constituting specific categories, and examples, of covered data:

- a government-issued identifier, such as a social security number, passport number, or driver's license number;
- any information that describes or reveals the past, presented, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual;
- a financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual;
- biometric information;
- genetic information;
- precise geolocation information;
- an individual's private communications, such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call, unless the covered entity or a service provider acting on behalf of the covered entity is the sender or an intended recipient of the communication;
- account or devices login credentials, or security or access codes for an account or device;
- information identifying the sexual behaviour of an individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of such information;
- calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of whether such information is stored on the individual's device or is accessible from that device and is backed up in a separate location;
- a photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual;
- information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a dedicated service;
- information about an individual when the covered entity or service provider has knowledge that the individual is a covered minor;
- an individual's race, colour, ethnicity, religion, or union membership;
- information identifying an individual's online activities over time and across third party websites or online services; and
- any other covered data collected, processed or transferred for the purposes of identifying all the abovementioned types of covered data.

In terms of exemptions, the following rules apply:

- communications, calendar information etc., are not private if such communications are made from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that such employer may access such communications;

- video content information used solely for transfers for independent video measurement;
- the last four digits of a debit or credit card number shall not be deemed sensitive covered data; and
- government-issued identifiers that are required by law to be displayed in public.

2.3. Data subject

California
Common also among the laws of Colorado, Connecticut, Utah, and Virginia, there is not an express definition of 'data subject' but instead a definition of 'consumer'. In this respect, the CCPA as amended defines 'consumer' as a natural person who is a California resident, however identified, including by any unique identifier.

Colorado
The CPA defines 'consumer' as an individual who is a Colorado resident and acts only in an individual or household context. If such an individual acts in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context, they fall outside the scope of this definition.

Connecticut
Similarly to the other state laws, with the exception of California, the CTDPA refers to 'consumer' as an individual who is a resident of Connecticut, but lists certain exceptions to this category which fall outside the scope of the definition. Specifically, an individual acting in a commercial or employment context does not fall under this definition of 'consumer'.

Iowa
The same definition is also found in the ICDPA, whereby a 'consumer' is defined as a natural person who is a resident of Iowa acting only in an individual or household context and excluding a natural person acting in a commercial or employment context.

Utah
The UCPA's definition of 'consumer' also refers to an individual who is a resident of Utah and is acting in an individual or household context, while excluding an individual acting in an employment or commercial context.

Virginia
Likewise, Virginia also defines 'consumer' as a natural person who is a resident of the Commonwealth acting only in an individual or household context, and explicitly excluding a natural person acting in a commercial or employment context.

USA Federal
The ADPPA does not explicitly define 'data subject', but refers to the term 'individual' throughout which is defined as 'a natural person residing in the US'. Individuals are also referred to as being linked or linkable to covered data. Additionally, 'employee' means an individual who is an employee, director, officer, staff member individual working as an independent contractor that is not a service provider, trainee, volunteer, or intern of an employer, regardless of whether such individual is paid, unpaid, or employed on a temporary basis.

2.4. Data controller

California

Similar to the definition of 'data subject' versus 'consumer', California does not define 'data controller' but instead defines 'business', which bears some similarity. Under this definition, which is quite detailed compared to the other state laws, a 'business' is a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organised or operated for the profit or financial benefit of its shareholders or other owners. It also collects consumers' personal information, or on the behalf of which such information is collected, and that alone, or jointly with others, determines the purposes and means of the processing of this personal information. However, the CCPA as amended adds additional requirements to be met to qualify as a 'business' regulated by the law, namely that such business must conduct its operations in California and satisfy one or more of the following thresholds:

- as of 1 January of any given calendar year, had annual gross revenues in excess of $25 million in the preceding calendar year;
- alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households; and
- derives 50% or more of its annual revenues from selling or sharing consumers' personal information.

Any entity that controls or is controlled by a business and that shares common branding with the business and with whom the business shares consumers' personal information, is also considered to be a business, with the CCPA as amended further defining what it means to 'control', be 'controlled', and 'common branding'.

A joint venture ('JV') or partnership composed of businesses in which each business has at least a 40% interest also falls within the definition of 'business'; however, the JV, partnership, and each business that composes the JV or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the JV or partnership shall not be shared with the other business.

Notably, the CCPA as amended also extends of the concept of business to any person that does business in California, and does not meet the requirements referred to above, that voluntarily certifies to the CPPA to be in compliance with, and agrees to be bound by, the CCPA as amended.

Colorado

Colorado takes a very simple approach, like Connecticut, Utah, and Virginia, providing that a 'controller' is a person that, alone or jointly with others, determines the purposes and means of processing personal data.

Connecticut

A 'controller' under the CTDPA is defined as an individual or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data.

Iowa

In the same vein, 'controller' under the ICDPA refers to a person that, alone or jointly with others, determines the purpose and means of processing personal data.

Utah

Utah's UCPA provides that a person who does business in Utah and who determines the purposes and means of processing personal data, regardless of whether they make the determination

alone or with others, is a 'controller', thereby following the same approach to this definition as Colorado, Connecticut, and Virginia.

Virginia
Pursuant to the CDPA, 'controller' is also to be understood as the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

USA Federal
The ADPPA does not utilise the terminology 'data processor', or 'data controller'. It does, however, describe the relationship between covered entities, large data holders, service providers, and third parties.

Most crucially, the ADPPA favours the term 'covered entity' to illustrate an entity or person, other than an individual but including any entity or person under its control, which:

- acts in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data;
- is subject to the FTC Act and is a common carrier under the Communications Act of 1934; and
- is an organisation which does not conduct business for its own profit or that of its members.

Service providers and public bodies, including that which acts on behalf of one, notably Federal, State, Tribal, territorial, or local government entities, are excluded from its definition.

Furthermore, it defines a 'large data holder' as a covered entity or service provider that, in the most recent calendar year:

- had annual gross revenues of $250 million or more; and
- collected, processed, or transferred:
  - the covered data of more than 5 million individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding covered data collected and processed solely for the purposes of initiating, rendering, billing for, finalising, completing, or otherwise collecting payment for a requested product or service; and
  - the sensitive covered data of more than 200,000 individuals or devices that identify or are linked, or reasonably linkable to one or more individuals.

Nevertheless, the definition for 'large data holder' excludes organisations which only collect or process personal email addresses, personal telephone numbers, or login information.

Additionally, the ADPPA expands even further with a definition of 'covered high impact social media company', which provides any internet-accessible platform generating over $3 billion in annual revenue and has 300 million or more monthly active users for not fewer than three of the preceding 12 months. Said company must also exist as an online product or service primarily used to access or share user-generated content.

2.5. Data processor

California
Similar to the approach taken for the definition of 'data controller', the CCPA as amended does not define 'data processor', but instead refers to 'service providers' and 'contractor'. A service provider is a person that processes information on behalf of a business and that receives from or on behalf of the business a consumer's personal information for a business purpose pursuant to a

written contract, provided that the contract prohibits certain things. Similarly, contractor means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided certain things are prohibited within the contract.

Colorado

Unlike California, Colorado does provide an express definition of 'processor' although it does not provide for an extensive definition. Instead, under the CPA the 'processor' is a person that processes personal data on behalf of a controller.

Connecticut

Similarly, Connecticut's CTDPA defines 'processor' as the individual who, or legal entity that, processes personal data on behalf of a controller.

Iowa

Like Colorado, Connecticut, Utah, and Virginia, Iowa adopts the same definition of 'processor', noting that a processor is the person who processes personal data on behalf of a controller.

Utah

Pursuant to the UCPA, the 'processor' is the person who processes personal data on behalf of a controller.

Virginia

Likewise, according to the CDPA, the term 'processor' means a natural or legal entity that processes personal data on behalf of a controller.

USA Federal

The ADPPA does not utilise the terminology 'data processor', or 'data controller'. It does, however, describe the relationship between covered entities, large data holders, service providers, and third parties. Accordingly, a 'service provider' may be either a person or an entity which collects, processes or transfers covered data on behalf of, and at the direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity, and receives covered data from or on behalf of the same entity.

Similarly, a 'third-party collecting entity' is defined as a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data and does not include a covered entity insofar as such entity processes employee data collected by an received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third party providing benefits to the employee. A third-party collecting entity cannot be defined as such if it is acting as a service provider.

Note that a large data holder may also be a service provider.

3. Legal basis

All state laws except for the ICDPA address consent as a legal basis for the processing of personal data, data outside of initially stated purposes, and sensitive data. Each differs slightly in how consent is presented. For example, California's CCPA as amended neither defines it nor directly addresses consent as a standalone legal basis. Contrastingly, the laws of Colorado, Connecticut, Utah, and Virginia each both define the term, and expressly provide it as a legal basis for certain processing of certain data types. Iowa, on the other hand, defines the term but does not clarify when or if it could be used as a legal basis.

They do, however, mirror each other to a certain degree with data subject contracts as a legal basis, with all laws not expressly addressing this but indirectly mentioning in the context of other provisions or limitations.

Legal obligation is a basis that the six laws have the most unity on, with use of almost identical language as well.

Public interest also shows some slight deviation, with five of the six laws addressing this as a legal basis, while Utah does not expressly address such a basis. With respect to the interest of controllers, here too we see some deviations between the six laws.

At a federal level, the ADPPA, if enacted, would outline that a covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is 'reasonably necessary and proportionate' to provide or maintain a specific product or service requested by the individual to whom the data pertains, or to effect one of the 17 permissible purposes outlined within the act. Interestingly, consent is not listed as a stand-alone purpose for processing and is instead a supplementary requirement for certain processing activities, including in relation to the use of internet search or browsing history for purposes of targeted advertising.

As with the six state-level laws, legal obligation is listed as a basis for processing under the ADPPA. The ADPPA also expressly references public interest as a permitted purpose.

As such, this section addresses five key legal basis and the differences between the six state privacy laws and the ADPPA, covering consent, data subject contract, legal obligations, public interest, and controller interest.

Please note that further information may be provided in supplementary regulations or guidance issued by regulatory bodies.

3.1. Consent

California

The CCPA as amended does not contain a single provision directly addressing consent but scatters this requirement across certain provisions within its text. Generally, and in the context of the CCPA as amended's right to opt-out, businesses are prohibited from selling consumers' personal information after its receipt unless the consumer subsequently provides express consent for the sale of the consumer's personal information. Additionally, the CCPA as amended defines 'consent' as any freely given, specific, informed and unambiguous indication of the consumer's

wishes. Notably, the CCPA as amended, similarly to Colorado and Connecticut, notes that with regard to consent:

- the acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent;
- hovering over, muting, pausing, or closing a given piece of content does not constitute consent; and
- agreement obtained through use of dark patterns does not constitute consent.

Furthermore, the CCPA as amended requires that businesses only use or disclose a consumer's sensitive personal information if the consumer subsequently provides consent for such use or disclosure for additional purposes.

Colorado

Colorado's CPA, like the other laws of California, Connecticut, Utah, and Virginia, expressly defines 'consent'. Specifically, consent under the CPA is a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement by which the consumer signifies agreement to the processing of their personal data.

Interestingly, the CPA also notes what does not constitute consent, which includes:

- acceptance of general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;
- hovering over, muting, pausing, or closing a given piece of content; and
- an agreement obtained through dark patterns.

In providing consent as a legal basis, the CPA also refers to consumer consent in the context of the right to opt-out, enabling the consumer to consent, with this consent taking precedence. Moreover, in controllers complying with their duties, the CPA expressly provides that controllers must comply with a duty to avoid secondary use unless they have gained consumer consent, as well as consent around the processing of sensitive data and its associated duty of care.

Connecticut

The CTDPA defines 'consent' as an affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer.

Connecticut follows Colorado in also providing what does not constitute consent, unlike the laws of Utah and Virginia. Notably, the CTDPA not only takes the same approach as Colorado, but in fact directly provides the same wording, noting that consent under the CTDPA would not include:

- acceptance of general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;
- hovering over, muting, pausing, or closing a given piece of content; or
- an agreement obtained through the use of dark patterns.

In terms of the use of consent as a legal basis, the CTDPA also provides that consent is required for processing of data for additional purposes, is needed for processing sensitive personal data, and details requirements around requiring consent if processing is for targeted advertising or the sale of personal data.

Iowa

Iowa's ICDPA, like the other laws of California, Colorado, Connecticut, Utah, and Virginia, provides a specific definition for 'consent' as a clear affirmative act signifying a consumer's freely given,

specific, informed, and unambiguous agreement to process personal data relating to the consumer, which may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

Uniquely, consent does not feature as a legal basis for processing in the ICDPA. Rather, the ICDPA mandates that clear notice and an opportunity to opt-out of processing be presented to consumers prior to the processing of their sensitive personal data.

Utah

The UCPA takes an approach to 'consent' that is more comparable to Virginia, in that it defines the term without noting circumstances that do not constitute consent. 'Consent' under the UCPA is defined as an affirmative act by a consumer that unambiguously indicates their voluntary and informed agreement to allow a person to process personal data related to them.

However, in the context of consent as a legal basis, the UCPA takes an approach more comparable to the CCPA as amended in that it does not provide detailed circumstances in which consent is required for processing. Instead, it more generally notes that consent is required for secondary processing purposes, and that sensitive data cannot be processed unless a consumer has first been given the opportunity to opt-out of such processing.

Virginia

Virginia takes the same approach as Utah in defining consent without providing circumstances that do not constitute consent, and defines this term as a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer.

It continues with this same approach taken by the other four state laws in requiring that consent be obtained for the processing purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as initially disclosed to the consumer. Concerning sensitive personal data, such data must also not be processing without obtaining consent.

USA Federal

As with most of the state laws, with the exception of the CCPA as amended, the ADPPA expressly defines consent, outlining that the term 'affirmative express consent' means an affirmative act by an individual that clearly communicates the individual's freely given, specific, informed, and unambiguous authorization for an act or practice, in response to a specific request from a covered entity that meets the requirements of subparagraph (B) (§2(1)(A) of the ADPPA).

Covered entities may not process covered personal data unless the processing is limited to what is 'reasonably necessary and proportionate' to provide or maintain a specific product or service requested by the individual whose covered data is being processed. Furthermore, processing is permitted under the ADPPA to achieve one of 17 other permissible purposes. Notably, however, consent is not included within the list of permissible purposes.

Instead, consent under the ADPPA is treated as a supplemental requirement for certain processing operations, not as a standalone basis for processing. As a result, consent alone will not legitimise processing activities not otherwise authorised under §101.

Under the ADPPA, affirmative express consent may be required before transferring certain types of covered data, including:

- sensitive covered data to third parties, unless another basis for the transfer applies;

- data that reveals the video content or services requested of an individual; and
- data of minors.

Consent may also be required if an organization wishes to retain data for longer than is required by law or for what is necessary for the purpose for which the data was collected, processed, or transferred.

The ADPPA also outlines that individuals should be given the opportunity to withdraw consent with regards to consent previously provided by the individual and in relation to changes to privacy policies.

3.2. Data subject contract

California

The CCPA as amended does not explicitly outline an obligation of a contract with respect to a data subject. However, and within the context of the right to deletion, the CCPA as amended provides that a business or service provider is not required to comply with a consumer's request to delete their personal information if it is necessary for, among other things, performing a contract between the business and the consumer.

Colorado

Similarly to California, Colorado also does not expressly provide a data subject contract as a legal basis for processing personal data. Instead, it more generally provides that controllers are not, in complying with the law, restricted in their ability to, among other things, provide a product or service pursuant to a contract with a consumer.

Connecticut

The CTDPA also does not expressly provide that personal data can be processed for the performance of a contract with a data subject. However, and like the other State laws, it states that its requirements do not restrict a controller or processor's ability to perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty and taking steps at the request of a consumer before entering a contract.

Moreover, the CTDPA's requirements do not restrict a controller or processor's ability to collect, use, or retain personal data to perform an internal operation that is reasonably aligned with the consumer's expectations based on their existing relationship with the controller, or otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or the performance of a contract to which they are a party.

Iowa

Iowa takes the same approach to the other state laws in not expressly providing a data subject contract as a legal basis for processing. Instead, it more generally provides that controllers are not, in complying with the ICDPA, restricted in their ability to, among other things, provide a product or service pursuant to a contract with a consumer, including written warranties, or taking steps at the request of the consumer or parent/guardian of a child prior to entering into a contract.

Furthermore, and comparable to the provisions under the CTDPA, UCPA, and CDPA, the ICDPA's requirements do not restrict a controller or processor's ability to process personal data to perform an internal operation that is reasonably aligned with the consumer's expectations, or anticipated, based on their existing relationship with the controller. The same applies if needed to aid the controller or processor in providing a product or service specifically requested by a consumer, parent, or legal guardian of a child or the performance of a contract to which they are a party.

Utah

Utah takes this same approach in not expressly providing a data subject contract as a legal basis for processing, but addressing such a contract in the controller and processor's obligations around taking steps requested or expected by a consumer. Specifically, the UCPA provides that its requirements do not restrict a controller or processor's ability to perform a contract to which the consumer or a child's parent or legal guardian is a party to, including fulfilling the terms of a written warranty or taking steps at the request of that individual before entering into the contract.

Moreover, and similarly to the comparable provision under Connecticut's CTDPA and Virginia's CDPA, the UCPA's requirements do not restrict a controller or processor's ability to process personal data to perform an internal operation that is reasonably aligned with the consumer's expectations based on their existing relationship with the controller. The same applies if needed to aid the controller or processor in providing a product or service specifically requested by a consumer, parent, or legal guardian of a child or the performance of a contract to which they are a party.

Virginia

Finally, Virginia too does not provide an express mention of data subject contracts as a legal basis for processing, but rather indirectly addresses this in a comparable manner to the other four state laws. Specifically, the CDPA cannot be construed to restrict a controller's or processor's ability to provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract.

Similarly, the obligations imposed on controllers or processors will not restrict their ability to collect, use, or retain data to perform internal operations that:

- are reasonably aligned with the expectations of the consumer;
- are reasonably anticipated based on the consumer's existing relationship with the controller; or
- are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

USA Federal

The ADPPA outlines that a covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to: (i) provide or maintain a specific product or service requested by the individual to whom the data pertains; or (ii) effect a purpose permitted under subsection (b).

As such, the ADPPA refers to 17 permissible purposes for processing data, including for the purpose of initiating, managing, or completing a transaction or fulfilling an order for specific products or services requested by an individual, such as any associated routine administrative, operational, and account-servicing activity such as billing, shipping, delivery, storage, and accounting. In addition, the ADPPA makes reference to contracts in relation to de-identified data and the collection, processing, and transfer of Social Security numbers.

3.3. Legal obligations

California

The CCPA as amended does address a business' legal obligations as a legal basis, noting that the obligations imposed under the CCPA as amended do not restrict a business' ability to:

- comply with federal, state, or local laws;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
- cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; and
- exercise or defend legal claims.

Colorado

Colorado takes a similar approach, noting that the obligations imposed under the CPA do not restrict a controller or processor's ability to:

- comply with federal, state, or local laws, rules, or regulations;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; or
- cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local law.

The CPA also addresses evidentiary privilege, noting that its provisions on controller and processor obligations do not apply where compliance would violate an evidentiary privilege under Colorado law. This same approach of addressing evidentiary privilege is seen in the other four state laws.

Connecticut

The same approach as is taken in Connecticut as the other four state laws, with the CTDPA providing that its requirements do not restrict a controller or processor's ability to, among other things:

- comply with a federal, state, or local law, rule, or regulation;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity;
- cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations; or
- investigate, establish, exercise, prepare for, or defend a legal claim.

The CTDPA also goes on to address evidentiary privilege, noting that it does not apply to the obligations imposed on controllers or processors where compliance would violate an evidentiary privilege under Connecticut law. Importantly, nothing in the CTDPA must be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Connecticut law as part of a privileged communication.

Iowa

Iowa takes a similar approach, where the ICDPA provides that nothing within its provisions should be construed to restrict a controller or processor's ability to:

- comply with federal, state, or local laws, rules, or regulations;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
- cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations; or
- investigate, establish, exercise, prepare for, or defend a legal claim.

Utah

The UCPA provides the same wording and requirements regarding legal obligations as a basis for processing data and compliance with its provisions, detailing that its requirements do not restrict a controller or processor's ability to:

- comply with a federal, state, or local law, rule, or regulation;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity;
- cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations; or
- investigate, establish, exercise, prepare for, or defend a legal claim.

Moreover, and like the other four privacy laws, it goes on the address evidentiary privilege. Specifically, the UCPA does not apply if a controller's or processor's compliance with the UCPA violates an evidentiary privilege under Utah law, or as part of privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Utah law.

Virginia

Finally, Virginia's CDPA follows the same approach as the other four laws in both provision and wording regarding legal obligations. It provides that nothing in its provisions must be construed to restrict a controller's or processor's ability to:

- comply with federal, state, or local laws, rules, or regulations;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities; or
- cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations.

It too addresses evidentiary privilege in the same manner, noting that the obligations imposed on controllers or processors will not apply where compliance would violate an evidentiary privilege under the laws of Virginia. Nothing in the CDPA must be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of Virginia as part of a privileged communication.

USA Federal

The ADPPA refers to 17 permissible purposes for processing data, including to comply with a legal obligation imposed by Federal, Tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider.

Furthermore, under the ADPPA, a covered entity may only transfer an individual's sensitive data to a third party in certain instances, including when the transfer is necessary to fulfil a legal obligation.

3.4. Public interest

California

Despite the other legal bases discussed above, the CCPA as amended expressly lists positive grounds for the general processing of personal information for the public interest. However, and with respect to processing and consumers' right to deletion, the CCPA as amended strikes out express reference to research in the 'public interest', and provides instead that a business or a service provider is not required

to comply with a consumer's request to delete personal information if it is necessary to maintain this information in order to engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws.

Colorado

Similarly, Colorado's CPA provides that the obligations imposed on controllers or processors do not restrict their ability to process personal data for reasons of public interest in the area of public health, but solely to the extent that the processing:

- is subject to suitable and specific measures to safeguard the rights of the consumer; and
- is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

Connecticut

Like Colorado, the CTDPA provides that its requirements do not restrict a controller or processor's ability to process personal data for reasons of public interest in the area of public health, community health, or population health, but solely to the extent that such processing is:

- subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and
- under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

Iowa

Iowa's ICDPA differs as it provides that the requirements imposed on controllers or processors do not restrict their ability to process personal data for engaging in public or peer reviewed scientific or statistical research in the public interest, subject to certain ethics and oversight conditions, including an oversight entity that determines the following:

- if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;
- the expected benefits of the research outweigh the privacy risks; and
- if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re- identification.

Furthermore, although its provisions do not expressly mention the 'public interest', the ICDPA notes that its requirements do not restrict processing in connection with:

- taking immediate steps to protect an interest that is essential for the life or physical safety of a consumer or another natural person, where the processing cannot be based on another legal basis; and
- preventing, detecting, protecting against, or responding to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity.

Utah

The deviation thus far with respect to public interest as a legal basis for processing is seen with Utah's UCPA. The reason for this is that the UCPA does not expressly address processing for the public interest, and instead focuses only on the interest of the data subject.

Virginia

Finally, Virginia follows the approach of California, Colorado, and Connecticut in providing that nothing in its provisions should be construed to restrict a controller's or processor's ability to engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable

ethics and privacy laws. This must also be approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine certain factors such as:

- whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;
- the expected benefits of the research outweigh the privacy risks; and
- if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

USA Federal
The ADPPA refers to 17 permissible purposes for processing data, including to:

- prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of 14 death, serious physical injury, or other serious health risk;
- conduct a public or peer-reviewed scientific, historical, or statistical research project that— (i) is in the public interest; and (ii) adheres to all relevant laws and regulations governing such research; and
- with respect to covered data previously collected in accordance with the ADPPA, a service provider acting at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, to prevent, detect, protect against or respond to a public safety incident, including trespass, natural disaster, or national security incident.

3.5. Data controller interest

California
Interestingly, the CCPA as amended does not expressly list positive grounds for the processing of personal information for the legitimate interest of the data controller.

Colorado
Colorado however, and in contrast to California, although not addressing the legitimate interest of controllers as a legal basis for processing, it indirectly provides that the CPA's obligation on controllers and processors do not restrict their ability to:

- prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity;
- preserve the integrity or security of systems; or
- investigate, report, or prosecute those responsible for any such action.

Connecticut
While Connecticut also does not expressly provide that personal data can be processed based on the legitimate interest of the data controller, it does address this indirectly like Colorado. Specifically, the CTDPA provides that its requirements do not restrict a controller or processor's ability to detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity. The same applies in order to investigate, report, or prosecute a person responsible for any of the aforementioned actions, as well as to assist another controller, processor, or third party with any of the obligations under the CTDPA.

Iowa
Similarly, Iowa does not address the legitimate interest of controllers as a legal basis for processing, it indirectly provides for the controller's interests, by stating that the ICDPA's requirements on controllers and processors do not restrict their ability to process data to:

- prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
- preserve the integrity or security of systems;
- investigate, report, or prosecute those responsible for any such action;
- conduct internal research to develop, repair, or improve products, services, or technology;
- effectuate a product recall;
- identify and repair technical errors existing or intended functionality; and
- assist another controller, processor, or third party with any of the obligations under this subsection.

Utah

While Utah takes a similar approach to Colorado and Connecticut in the circumstances to be indirectly considered the legitimate interest of the controller (as opposed to a direct provision addressing this), it is slightly more limited in scope. As such, the UCPA provides that its requirements do not restrict a controller or processor's ability to detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity, or to investigate, report, or prosecute a person responsible for any of the aforementioned actions. The same applies in order for the controller or processor to preserve the integrity or security of systems, or to investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems.

Virginia

Finally, although the CDPA also does not directly address the legitimate interest of controllers, it does provide some slightly different circumstances that those under the laws of Colorado, Connecticut, and Utah. Specifically, nothing in the CDPA should be construed to restrict a controller's or processor's ability to investigate, establish, exercise, prepare for, or defend legal claims. In addition, the obligations imposed on controllers or processors must not restrict their ability to collect, use, or retain data to:

- conduct internal research to develop, improve, or repair products, services, or technology;
- effectuate a product recall;
- identify and repair technical errors that impair existing or intended functionality; or
- perform certain internal operations.

USA Federal

While the ADPPA does not expressly refer legitimate interest as a legal basis, it does list 17 permissible purposes for processing data, which include collecting, processing or transferring data:

- to initiate, manage, or complete a transaction or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account-servicing activity such as billing, shipping, delivery, storage, and accounting;
- information previously collected in accordance with the ADPPA, or for processing necessary to perform system maintenance or diagnostics or to develop, maintain, repair, or enhance a product or service for which such data was collected, to conduct internal research or analytics to improve a product or service for which such data was collected, to perform inventory management or reasonable network management, to protect against spam, or to debug or repair errors that impair the functionality of a service or product;
- to authenticate users of a product or service;
- to fulfill a product or service warranty;
- to prevent, detect, protect against, or respond to a security incident;
- to prevent, detect, protect against, or respond to fraud, harassment, or illegal activity;
- to prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of death,

serious physical injury, or other serious health risk;

- to effectuate a product recall pursuant to Federal or State law;
- to conduct a public or peer-reviewed scientific, historical, or statistical research project that— (i) is in the public interest; and (ii) adheres to all relevant laws and regulations governing such research;
- to deliver a communication that is not an advertisement to an individual, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity;
- to deliver a communication at the direction of an individual between such individual and one or more individuals or entities;
- to ensure the data security and integrity of covered data, as described in §208; and
- with respect to covered data previously collected in accordance with the ADPPA, a service provider acting at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, to prevent, detect, protect against or respond to a public safety incident, including trespass, natural disaster, or national security incident.

4. Controller and processor obligations

While all six of the State privacy laws and the ADPPA do not directly address the cross-border transfer of personal data, they do instead somewhat address the sale/sharing of data with third parties. Nevertheless, and with the exception of California, the other five State laws continue to adopt a unified approach in their provisions, referring to data transfer and disclosure to third parties and affiliates of the controller indirectly. Likewise, the ADPPA, though not providing explicit rules relating to cross-border transfers, does require cross-border transfers to occur under the general permissible purposes for transferring data.

Record keeping requirements, on the other hand, present a much clearer divide with California and Connecticut containing some provisions, although very limited, while the other four States and the ADPPA are silent on any such requirements.

Regarding risk assessments, although the different laws take different approaches and use differing terminology such as 'risk assessment', 'data protection assessment', or 'privacy risk assessment' for example, they largely provide similar requirements in great detail as in the ADPPA, with the exception of Utah and Iowa which are entirely silent on the matter.

Security and breaches are also addressed in much the same way across the state laws, with the exception of the ADPPA and Iowa which do not address security breaches, although the ADPPA does provide for general security requirements for processing. The reason being that most States provide for breach requirements in a separate statute, and do not address the matter directly within the comprehensive privacy laws. They do, however, provide for controller and processor data security requirements, with both the provision and wording being very similar.

Although the state laws are unified in all containing obligations with respect to third parties and vendor contracts, the provisions themselves differ slightly. Colorado, Connecticut, Iowa, Utah, Virginia, and the ADPPA take a common approach in both obligation and wording, while California provides more detailed information.

Finally, all of the state laws and the ADPPA address requirements of a privacy policy and informing consumers in detail, although the laws of Colorado, Connecticut, Iowa, Utah, and Virginia continue in providing matching provisions, with California deviating somewhat.

As such, here too we see a varied approach between the State laws, as well as the federal legislation. The section below therefore provides how each of the state laws and the federal law addresses various controller and processor obligations, focusing on data transfers and sharing, record keeping requirements, risk assessments, security and breaches, third parties and vendor contracts, and privacy policies.

Please note that further information may be provided in supplementary regulations or guidance issued by regulatory bodies.

4.1. Data transfers/data sharing

California

The CCPA does not contain provisions explicitly relating to cross-border data transfers and localisation. Instead, it addresses the transfer and sharing of information with third parties, by including the transferring of data to third parties in the definition of selling and sharing. In this respect, selling is defined as the selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary or other valuable consideration whereas sharing means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross context behavioural advertising for the benefit of a business In which no money is exchanged. The CCPA also details what would not constitute the selling and sharing of personal information, but the aforementioned definition provides a good understanding of which business activities would fall within this definition and therefore constitute a transfer or sharing.

In addition, and in accordance with a consumer's right to opt out, consumers have the right to choose not to have their data shared with third parties, and although businesses may offer financial incentives to sell personal information, such incentives must be disclosed, and businesses must be transparent about this practice.

Colorado

Like California, Colorado's law also does not address the cross-border transfer of data, but instead focuses on the sale or sharing of data with third parties. However, unlike California, Colorado takes a very indirect approach in addressing this, and relates it to de-identified data and activities that controllers and processors are not required to take.

Specifically, and regarding de-identified data, the CPA provides that controllers are not required to comply with an authenticated consumer rights request if they do not sell personal data to any third party or otherwise voluntarily disclose the personal data to any third party, except if the consumer authorises this, among other cumulative criteria which must be met. As such, we can see that the CPA is silent on the topic of both cross-border transfers, and to a large degree, the direct address of sharing or selling personal data and any such associated obligations.

Connecticut

Similarly, the CTDPA also does not provide for requirements for cross border data transfers, and instead only addresses the disclosure and sharing of personal data with third parties, but does so in the context of potential violations of the CTDPA following any such disclosure. So again, the CTDPA remains largely silent on any requirements around the transfer or sharing of data.

With respect to potential CTDPA violations post-disclosure, the CTDPA only stipulates that a controller or processor disclosing personal data to another processor or third-party controller will not be deemed to have violated the CTDPA if this new processor or third-party controller violates the CTDPA, provided that at the time of disclosure, the original processor or controller did not have actual knowledge that the receiving processor or third-party controller would violate the CTDPA.

Iowa

Notably, the ICDPA does not address obligations for cross-border data transfers. However, the ICDPA does note that the 'sale of personal data' does not include, among other things:

- the disclosure or transfer of personal data to an affiliate of the controller;
- 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; or
- 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.

The ICDPA provides, in relation to privacy notices, that the categories of third parties, if any, with whom the controller shares personal data should be outlined to consumers.

Utah

Contrastingly, the UCPA entirely does not address obligations for cross-border data transfers, nor for disclosure or sharing, but instead outlines what does not constitute sale of personal data, and more generally noting that consumer authorisation is needed for any disclosure.

Virginia

Finally, Virginia follows suit and also does not address any cross-border data transfer requirements, also only outlines what does not constitute sale of personal data by addressing certain types of disclosures, and providing the same provision regarding potential violations following any disclosure to a third party as we see in Connecticut's CTDPA.

USA Federal

The ADPPA does not explicitly contain provisions regulating cross-border data transfers, but does define transfers as disclosing, releasing, disseminating, making available, licensing, renting, or sharing covered data orally, in writing, electronically or by any other means. Generally, the ADPPA provides that the transfers may occur under the permissible purposes provided, and also adds exceptions to prohibition on the transfer of individuals sensitive covered data. Likewise, covered entities may not transfer the covered data of a covered minor to a third party, if the covered entity has knowledge that the individual is a covered minor and has not obtained affirmative consent from the covered minor.

However, the ADPPA does provide that covered entities must provide for the right to opt-out of data transfers to third parties, and describes under §210 of the ADPPA, the opt-out mechanism that must be establish to facilitate this right.

4.2. Data processing records

California

The CCPA as amended provides business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal Information of a consumer who submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under the CCPA as amended. In addition, the CCPA as amended states that the CPPA can create regulation specifying record keeping requirements for businesses to ensure compliance with the same.

Colorado

Contrastingly, Colorado's CPA is entirely silent on obligations around record-keeping, and does not provide for data processing record requirements.

Connecticut

Connecticut on the other hand, takes an approach between that of California and Colorado. While the CTDPA does not expressly provide for record-keeping requirements, it addresses the maintenance of a record associated with a consumer's deletion request. Specifically, the CTDPA

provides that controllers obtaining personal data from a source other than the consumer, will be in compliance with a consumer's request to delete by retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the personal data remains deleted, and not using such retained data for any other purpose.

Iowa
Similarly to Colorado, Iowa's law does not provide for data processing record requirements.

Utah
Utah on the other hand, takes the same approach as Colorado in neither addressing directly or indirectly, requirements for maintain processing records or any other record-keeping requirements.

Virginia
Similarly, the CDPA also does not expressly provide for record-keeping requirements.

USA Federal
The ADPPA does not contained any requirements to maintain records of processing activities by covered entities or service providers.

4.3. Risk assessments

California
California's CCPA as amended establishes requirements around 'risk assessments', and mandating the CPPA with the authority to issue regulations on the matter. Specifically, businesses whose processing of consumers' personal information present significant risks to privacy or security, would be required to regularly submit a risk assessment with respect to their processing activities, including whether these involve sensitive personal information. They would further be required to identify and weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer, with the ultimate goal of restricting or prohibiting such processing if the risks outweigh the benefits.

Colorado
Colorado also directly addresses obligations around conducting 'data protection assessments', by requiring controllers not to carry out processing activities that present heightened risk of harm to a consumer, without first conducting and documenting a data protection assessment of each of its processing activities. The CPA further establishes what would, in this context, qualify as a heightened risk, noting that this includes:

- processing for purposes of targeted advertising or profiling if the profiling presents a reasonably foreseeable risk of:
  - unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
  - financial or physical injury to consumers;
  - a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
  - other substantial injury to consumers;
- selling personal data; and
- processing sensitive data.

In addition, and similarly to the CPRA, the CPA notes that such data protection assessments must identify and weigh the benefits of the processing against the potential risks, as mitigated by safeguards that the controller can employ to reduce the risks, and must also factor into these

assessments the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed.

Such assessments also need to be made available to the Attorney General ('AG') upon request, with the AG able to further assess compliance with the obligations under the CPA. Interestingly, a single data protection assessment may also be used address a comparable set of processing operations that include similar activities. However, as the CPA has not yet taken effect, data protection assessment requirements apply to processing activities created or generated after 1 July 2023 and are not retroactive.

Connecticut

Similarly, the CTDPA also expressly provides controllers with an obligation to conduct and document 'data protection assessments' for each of their processing activities that presents a heightened risk of harm to a consumer. It also goes on the share the same wording in this requirement as Colorado, noting that heightened risk of harm to a consumer includes:

- processing for the purposes of targeted advertising;
- sale of personal data;
- processing for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of:
  - unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
  - financial, physical, or reputational injury to consumers, a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
  - other substantial injury to consumers; and
- the processing of sensitive data.

In addition, the CTDPA also requires that such assessments identify and weigh the benefits against the potential risks, and require the controller to factor into any such assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed. A single DPIA may also address a comparable set of processing operations that include similar activities, must be made available to the AG, and also only apply to processing activities created or generated after 1 July 2023, at which point to CTDPA takes effect, and are not retroactive, as we see in Colorado.

Iowa

Notably, Iowa deviates from the majority of the other State laws, in that it does not require controllers to conduct data protection assessments, or other risk assessments.

Utah

Utah also deviates from the standard of containing a requirement around impact assessments. As such, the UCPA is silent on this, and does not provide for data protection or privacy impact assessment requirements.

Virginia

Finally, Virginia takes a similar approach to California, Colorado, and Connecticut in containing a requirement for data controllers to conduct and document data protection assessments. Specifically, the CDPA requires such assessments for activities which involve:

- processing of personal data for purposes of targeted advertising;
- sale of personal data;

- processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:
  - unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
  - financial, physical, or reputational injury to consumers;
  - a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
  - other substantial injury to consumers;
- processing of sensitive data; and
- any processing activities involving personal data that present a heightened risk of harm to consumers.

The CDPA continues to mirror some of the additional requirements as provided by Colorado and Connecticut, and requires that data protection assessments be confidential, identify and weigh the benefits against the potential risks, with controllers considering and factoring in the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed. They must also be available to the AG, can address a comparable set of processing operations that include similar activities within one single assessment, and apply to processing activities created or generated after 1 January 2023, when the CDPA will enter into effect, and are not retroactive.

USA Federal

The ADPPA requires that a privacy impact assessment ('PIA') be conducted under various circumstances. Firstly, the ADPPA provides that covered entities establish, implement, and maintain policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transfer of covered data, including considering applicable Federal laws, rules or regulations related to covered data, and identify, assess and mitigate privacy risks related to covered minors.

In addition, the ADPPA specifies that large data holders, who use a covered algorithm whch poses a consequential risk of harm to an individual or group of individuals, must conduct PIAs once every two years. Although, PIAs must initially be conducted within one year of being defined as such or within one year after the date of enactment of the ADPPA, which is earlier, PIAs are required biennially following this.

More specifically, the ADPPA outlines that PIAs for covered algorithms include:

- a detailed description of the design process and methodologies of the covered algorithm;
- a statement of the purpose and proposed uses of the covered algorithm;
- a statement of the purpose and proposed uses of the covered algorithm;
- a description of the data used including the specific categories of data that will be processed as input and any data used to train the model that the covered algorithm relies on;
- a description of the outputs produced by the covered algorithm;
- an assessment of the necessity and proportionality of the covered algorithm in relation to its stated purpose; and
- a description of the steps taken or steps that will be taken to mitigate potential harms from the covered algorithm to an individual or group of individuals.

Furthermore, the ADPPA notes that a covered entity and a service providers, no later than 30 days after completing a PIA of a covered algorithm, submit the PIA to the Commission, upon request make the PIA available to Congress, and make a summary of the PIA available in a place that is easily accessible to individuals.

4.4. Data security and breaches

California

To the extent that we consider obligations around data breaches, the CCPA as amended itself does not address this topic, breach notification, like in most other US States, is regulated in other statutes as opposed to comprehensive privacy laws. In this respect, California law does require the notification of breaches, with such requirements detailed in the California Civil Code.

However, the CCPA as amended reinforces the breach notification obligations under the California Civil Code, stipulating that a business should be held directly accountable to consumers for data security breaches and must notify consumers when their most sensitive information has been compromised. In addition, the CCPA as amended stipulates that businesses should be held directly accountable to consumers for data security breaches and must notify consumers when their most sensitive information has been compromised.

Furthermore, the CCPA as amended contain provisions providing for consumer relief for data breaches, although this does not expressly contain requirements for controllers in the event of a breach.

Colorado

The CPA takes a similar approach, as with most US states, in regulating breach requirements outside of the CPA through a dedicated part of the statute.

The CPA does, however, provide controller obligations with respect to data security practices. In this regard, the CPA requires controllers to abide by a duty of care, where they must take reasonable measures to secure personal data, and where such measures must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business itself. The CPA also establishes associated requirements for processors in this regard, where they too must assist controllers in their obligations around maintaining security and responding to breaches.

Finally, and the provision that appears most common in the comprehensive privacy laws of Colorado, Connecticut, Utah, and Virginia, is the express requirement for controllers and processors to implement appropriate technical and organisational measures to ensure a level of security which is appropriate to the risk, and to establish a clear allocation of the responsibilities in this regard.

Connecticut

Likewise, the CTDPA does not provide for breach notification requirements as these are contained in another part of Connecticut's statute, but does address data security obligations.

Specifically, controllers are required to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue. We can see that the language here is quite similar to that of Colorado, Utah, and Virginia.

Processors have a similar requirement, where they must assist the controller in meeting their obligations, including obligations related to the security of processing personal data and notification of a breach of the security system.

Iowa

Similar to the requirements in all other State laws, the ICDPA stipulates that controllers must adopt and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity and accessibility of personal data. Notably, the ICDPA provides that such data

security practices must be appropriate to the volume and nature of the personal data at issue.
In addition, the ICDPA notes similar requirements for processors, in assisting controller's in meeting their obligations, namely in relation to the security of processing and the notification of a security breach of the processor.

Utah

Utah also addresses its breach notification requirements in a separate statute and not within the UCPA, but does address controller and processor data security requirements, and does so in the same way as Colorado, Connecticut, and Virginia.

As such, processors are required to assist controllers in meeting their obligations, including obligations related to the security of processing personal data and notification of a breach of security system. Meanwhile, controllers have the initial obligation of establishing, implementing, and maintaining reasonable administrative, technical, and physical data security practices designed to protect the confidentiality and integrity of personal data, and to reduce reasonably foreseeable risks of harm to consumers.

Virginia

Finally, Virginia also addresses its breach notification obligations outside of the CDPA itself, but does expressly provide for controller and processor obligations for data security measures. In this respect, processors must assist controllers in meeting obligations in relation to the security of data processing, and in relation to the notification of a breach of security. Meanwhile, the CDPA follows the same approach in requirement and wording as Colorado, Connecticut, and Utah in requiring controllers to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, where such practices must be appropriate to the volume and nature of the personal data at issue.

USA Federal

The ADPPA does not contain any requirements for a data breach notification to the Commission or data subjects.

However, the ADPPA does provide that a covered entity or service providers, establish, implement, and maintain reasonable administrative, technical and physical data security practices and procedures to protect and secure covered data against unauthorised access and acquisition. In considering such practices, the ADPPA provides such practices be appropriate to, among other things, the size and complexity of the covered entity or service providers, the nature and scope of the collection, processing, or transfer of covered data, the sensitivity of the covered data, current state of the art of safeguards for protecting covered data, and the cost of available tools to improve security and reduced vulnerabilities in relation to the risks and nature of covered data.

In addition, the ADPPA outlines, in detail, the minimum data security practices required of covered entities. These include:

- assessment of vulnerabilities, including internal and external risk to each system maintained by the covered entity;
- taking preventive and corrective action to mitigate reasonably foreseeable risks or vulnerabilities;
- evaluating preventive and corrective actions in light of material changes in technology, internal or external threats, and changing business arrangements or operations;
- disposing of covered data in accordance with a retention schedule that requires the deletion of covered data;
- training of employees with access to covered data on how to safeguard covered data and updating the training as necessary;

- designating an officer, employee or employees to maintain and implement such practices; and
- implementing procedures to detect, respond to, or recover from security incidents, including breaches.

4.5. Third party/vendor contract requirements

California

While the CCPA as amended does not contain a standalone provision directly addressing and requiring a contract to be in place between controllers, third parties, service providers, and contractors, there is an indirect requirement to conclude an agreement with such entities in line with the definitions of service provider and contractors. Specifically, the definitions of service providers and contractor outline what should be prohibited in contracts with such entities including:

- selling or sharing the personal information;
- retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract; and
- retaining, using, or disclosing the information outside of the direct business relationship.

Additionally, the CCPA as amended allows for the business to monitor the service provider's compliance with the contract through measures including ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every 12 months.

Finally, the CCPA as amended also addresses the obligation of an agreement being in place in the case that a business collects a consumer's personal information and sells that personal information to, or shares it with, a third party or discloses it to a service provider or contractor. In such a case, an agreement must be in place, with this agreement:

- specifying that the personal information is sold or disclosed by the business only for limited and specified purposes;
- obligating the third party, service provider, or contractor to comply with applicable obligations under the CCPA as amended and to provide the same level of privacy protection as is required by the CCPA as amended;
- granting the business rights to take reasonable and appropriate steps to ensure that the transferred personal information is used in a manner consistent with the business' obligations under the CPRA;
- requiring the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under the CCPA as amended; and
- granting the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorised use of personal information.

Colorado

The CPA follows in the steps of California, but differs in that obligations around a contract between controllers and processors is directly detailed as a standalone provision. As such, the CPA details that processing by a processor must be governed by a contract, with this contract setting out the processing instructions, the type of personal data subject to the processing, the duration of processing, and any additional obligations to be complied with in assisting the controller with their obligations.

If the processors wishes to engage a subprocess, there too a contract must be in place, although the controller must first be informed and given the opportunity to object.

Nevertheless, the CPA notes that in no event may a contract relieve a controller or a processor from the

liabilities imposed on them by virtue of their roles in the processing relationship.

Connecticut

Likewise, Connecticut also requires a contract to be in place between controllers and processors, as well as subcontractors. This contract should clearly set forth instructions for processing data, the nature and purpose of processing, the type of data which is subject to processing, the duration of processing, and the rights and obligations of both parties. It also needs to require the processor to:

- ensure each person processing personal data is subject to a duty of confidentiality;
- at the controller's direction, delete or return all personal data, unless retention is required by law;
- make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations of the CTDPA;
- engage any subcontractor pursuant to a written contract with the same obligations; and
- cooperate with reasonable assessments by the controller.

Iowa

The ICDPA is similar to the other privacy laws, in containing obligations for processor contracts, but more generally also notes that processor's must assist controllers in their duties required under the ICDPA, taking into account the nature of processing and the information available to the processor by appropriate and technical and organisational measures, insofar as reasonable practicable:

- to fulfil the controller's obligation to respond to consumer rights requests; and
- to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a security breach of the processor.

More specifically, the ICDPA requires a contract between controllers and processors which clearly sets forth instructions for processing personal data, the duration of processing, the type of data subject to processing, the duration of processing, and the rights and duties of both parties.

Controller-processor contracts must also ensure:

- each person processing personal data is subject to a duty of confidentiality with respect to the data;
- at the controller's direction, delete or return all of the personal data to the controller as requested at the end of the provision of services, unless retention of personal data is required by law;
- upon reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations under the ICDPA;
- engage any subcontractor or agent pursuant to a written contract in accordance with the obligations set out above, that requires the subcontractor to meet the duties of the processor with respect to personal data.

Utah

Like the other requirements discussed in the other five privacy laws, the UCPA also contains obligations around processor contracts, requiring such a contract to be in place between controllers and both processors and subcontractors, which:

- clearly sets forth:
  - instructions for processing personal data;
  - the nature and purpose of the processing;
  - the type of data subject to processing;
  - the duration of the processing; and
  - the parties' rights and obligations;
- requires the processor to ensure each person processing personal data is subject to a duty of

confidentiality with respect to the personal data; and
- requires the processor to engage any subcontractor pursuant to a written contract with the same obligations.

Virginia

Finally, Virginia is no different, and requires data processors to adhere to the instructions of a controller and assist the controller in meeting its obligations under the CDPA. To facilitate this, the CDPA provides that a contract between a controller and a processor must govern the processor's data processing procedures, will be binding, and must clearly set forth:

- instructions for processing 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 must also include requirements that the processor:

- ensure that each person processing personal data is subject to a duty of confidentiality;
- at the controller's direction, deletes or returns all personal data to the controller, unless retention is required by law;
- makes available to the controller all information necessary to demonstrate the processor's compliance with the obligations in the CDPA;
- allows reasonable assessments by the controller or arranges for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organisational measures in support of the obligations under the CDPA;
- provides a report of such assessment to the controller upon request; and
- engages any subcontractor pursuant to a written contract with the same obligations.

USA Federal

While the ADPPA does not contain a standalone provision directly addressing and requiring a contract to be in place between covered entities and service providers, service providers are required to follow the same obligations as covered entities in processing personal data. In particular, a service provider is defined as a person or entity that collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity, for the purpose of allowing the service provider to perform a service of function on behalf of, and at the direction of such covered entity. Although, the obligations surrounding de-identified data are required to be included contractually in all subsequent instances for which data may be received.

However, the ADPPA does outline specific obligations of third party collecting entities. Namely, the ADPPA notes that each third party collecting entity must place a clear, conspicuous, not misleading and readily accessible notice on the website or mobile application of the third-party collecting entity. This must notify individuals the entity is a third party collecting entity, include a link to the website, and be reasonably accessible to and usable by individuals with disabilities.

4.6. Privacy policies

California

A business is required to disclose and update annually the following information in the form of its online privacy policy and if the business does not maintain those policies, on its internet website:
- a description of a consumer's rights, and one or more designated methods for submitting requests;

- a list of the categories of personal information collected about consumers in the preceding 12 months that most closely describe the personal information collected; and
- two separate lists for:
  - a list of the categories of personal information it has sold about consumers in the preceding 12 months that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business must disclose that fact; and
  - a list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business must disclose that fact.

Colorado

Colorado requires controllers to, in complying with their duty of transparency, to provide a reasonably accessible, clear, and meaningful privacy notice that includes:

- the categories of personal data collected or processed by the controller or a processor;
- the purposes for which the categories of personal data are processed;
- how and where consumers may exercise their rights, including the controller's contact information and how to appeal a controller's action with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with whom the controller shares personal data; and
- if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing.

Connecticut

Similarly, and in line with the wording of the other five privacy laws, Connecticut also requires controllers to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

- the categories of personal data processed by the controller;
- the purpose for processing personal data;
- how consumers may exercise their consumer rights, including how to appeal a controller's decision with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with whom the controller shares personal data; and
- an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

In addition, where a controller sells personal data to third parties or processes personal data for targeted advertising, they must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise their right to opt out of such processing.

Iowa

Iowa takes the same approach as the other State privacy laws, in stipulating that controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice, and that it must include:

- the categories of personal data processed by the controller;
- the purpose for processing personal data;
- how consumers may exercise their consumer rights including how a consumer may appeal a controller's decision with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any; and

- the categories of third parties, if any, with whom the controller shares personal data.

Similar to other State privacy laws, the ICDPA also requires controllers which sell consumer data to third parties or that engage in targeted advertising, to clearly and conspicuously disclose such activities in the privacy notice, as well as the manner in which consumer's may exercise their right to opt-out of such processing.

Building on the above, the ICDPA requires controllers to establish, and describe in the privacy notice, secure and reliable means for consumers to submit requests to exercise their consumer's rights.

Utah

Utah continues to take this same approach as Colorado, Connecticut, and Virginia, and requires controllers are required to provide consumers with a reasonably accessible and clear privacy notice and inform them of:

- the categories of personal data processed by the controller;
- the purposes for which the categories of personal data are processed;
- how consumers may exercise a right;
- the categories of personal data that the controller shares with third parties, if any; and
- the categories of third parties, if any, with whom the controller shares personal data.

Additionally, if data is sold to one or more third parties or the controller engages in targeted advertising, they must clearly and conspicuously disclose to the consumer the manner in which the consumer can exercise their right to opt out of the sale of their personal data or the processing for targeted advertising.

Virginia

Finally, and as seen in the privacy laws of Colorado, Connecticut, and Utah, Virginia contains the same provision around its privacy policy, following a similar wording as well, and requires the privacy policy to be reasonably accessible, clear, and meaningful, and to include:

- the categories of personal data processed by the controller;
- the purpose for processing personal data;
- how consumers may exercise their rights, including how to appeal a controller's decision with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any; and
- the categories of third parties, if any, with whom the controller shares personal data.

In addition, if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

USA Federal

The ADPPA provides that each covered entity must make publicly available, in a clear conspicuous, not misleading, and easy-to-read and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity.

The contents of the privacy policy of the covered entity must include:

- the identity and contact information of:
  - the covered entity or service provider to which the privacy policy applies, including points of contact and generic email addresses for privacy and data security inquiries;
  - any other entity within the same corporate structure as the covered entity or service provider to

which covered data is transferred by the covered entity;
- the categories of covered data the covered entity or service provider processes;
- the processing purposes for each category of covered data the covered entity or service provider collects or processes;
- whether the covered entity or service provider transfers covered data and if so, each category of service provider or third party to which data is transferred, the name of each third party, and purposes for which data is transferred to categories of service provider or third party;
- the length of time data is intended to be retained, for each category of data, or if not possible to identify that timeframe the criteria used to determine the length of time to retain categories of covered data;
- a prominent description of how an individual can exercise their rights under the ADPPA;
- a general description of security covered entities or service providers security practices;
- the effective date of the privacy policy; and
- whether or not any covered data collected is transferred, processed, stored, or otherwise accessible in the People's Republic of China, Russia, Iran, or North Korea.

Furthermore, the privacy policy must be made available to the public in each covered language in which the covered entity or service provider provides a product or service that is subject to the privacy policy, or carries out activities related to the product or service. Access must also be provided in a manner reasonably accessible to and usable by individuals with disabilities.

In addition, where the privacy policy makes a material change to its privacy policy or practices, the covered entity must notify each individual affected by the material change and provide an opportunity to withdraw consent to any further materially different collection, processing, or transfer. In notifying individuals, the covered entity or service provider must provide a notification in a covered language.

More specifically, large data holders must retain copies of previous versions of their privacy policy for at least 10 years beginning after the date of the enactment of the ADPPA, and publish such previous policies on their website. Likewise, large data holders must include a log describing the date and nature of each material change to their privacy policy over the past 10 years, with descriptions sufficient for a reasonable person to understand the material effect of each material change.

5. Data subject rights

As with many other provisions between the six state comprehensive privacy laws, the provisions regarding data subject rights take a similar approach in providing a unified approach when it comes to Colorado, Connecticut, Iowa, Utah, and Virginia, with California deviating slightly in both approach and wording. Firstly, and regarding the right to be informed, California makes a separation between informing individuals in instances where data is collected, and instances where data is sold or shared, instead of providing one common provision as we see with Colorado, Connecticut, Iowa, Utah, and Virginia. As it concerns the other five States, they largely follow the same language to each other, with the right to be informed being presented within the obligation to provide a privacy policy, as is discussed in the section on obligations above.

The right of access, in contrast, takes a much less detailed approach in the provisions within California, Colorado, Connecticut, Iowa, Utah, and Virginia's laws. Specifically, the laws note a right of access, but do not provide any additional requirements or considerations specific to that right. The same approach is taken across the four state comprehensive privacy laws for the right to rectification, erasure, objection or opt-out, not to be subject to automated decisions-making, and portability, with the exception of Utah and Iowa, which do not provide a right not to be subject to automated decision-making. Furthermore, Utah also does not provide an express right to rectification.

However, with respect to the right not to be subject to automated decision-making, California addresses the matter under the CCPA as amended, while Colorado, Connecticut, Utah, and Virginia address the right indirectly as an opt-out option within the right to opt-out of certain processing.

At federal level, the ADPPA, if enacted, would establish a comprehensive set of individuals' rights on all accounts, which are generally wider in scope and in detail than those under state law. For example, rights to rectification and erasure under the ADPPA also require covered entities to notify third parties or service providers to which a data subject's personal data has been transferred. Furthermore, while the state laws refer to the right to opt out of the sale of personal data, the ADPPA provides for the right to opt out of all transfers, whether or not for profit. Notably, although the ADPPA does not explicitly address automated decision-making, it confers certain civil rights protections in relation to discrimination and algorithms. The ADPPA also requires the FTC to develop unified opt-out mechanisms.

As such, the section below highlights the similarities and differences between the laws of California, Colorado, Connecticut, Iowa, Utah, Virginia, and the ADPPA with respect to data subjects' right to be informed, to access, correct, delete, personal data, opt-out of certain processing, as well as rights to data portability and not being subject to automated decision-making.

Please note that further information may be provided in supplementary regulations or guidance issued by regulatory bodies.

5.1. Right to be informed

California

In line with the other US State privacy laws, the CCPA as amended details specific information to be provided to consumers at or before the point of collection.

Specifically, a business that controls the collection of consumer's personal information must, at or before the point of collection, inform consumers of:

- the categories of personal information to be collected;
- the purposes for which the categories of personal information are collected or used and whether such information is sold or shared; and
- the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period.

In regard to sensitive data, a business must provide the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared.

Colorado

In line with the CCPA as amended, the CPA requires controllers to provide consumers with a privacy notice that includes:

- the categories of personal data collected or processed by the controller or a processor;
- the purposes for which the categories of personal data are processed;
- how and where consumers may exercise their rights, including the controller's contact information and how a consumer may appeal a controller's action with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with whom the controller shares personal data; and
- if a controller sells personal data to third parties or processes personal data for targeted advertising, to clearly and conspicuously disclose the sale or processing, as well as how a consumer may exercise the right to opt out of such sale or processing.

Connecticut

Similarly, the CTDPA stipulates that consumers have the right to confirm whether a controller is processing their personal data. Additionally, controllers are required to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

- the categories of personal data processed by the controller;
- the purpose for processing personal data;
- how consumers may exercise their rights, including how they may appeal a controller's decision with regard to their request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with whom the controller shares personal data;
- an active electronic mail address or other online mechanisms that the consumer may use to contact the controller; and
- where a controller sells personal data to third parties or processes personal data for targeted advertising, to clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

Iowa

Similar to the CPA, consumers have the right to confirm whether a controller is processing their personal data. Controllers must provide consumers with a reasonably accessible, clear and meaningful notice that includes the following:

- the categories of personal data processed by the controller;
- the purpose for processing personal data;

- how consumers may exercise their consumer rights pursuant to §715D.3 of the ICDPA, including how a consumer may appeal a controller's decision with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with whom the controller shares personal data.

In addition, the ICDPA requires that if a controller sells a consumer's personal data to third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity.

Furthermore, the ICDPA requires controllers to establish and describe in a privacy notice, secure and reliable means for consumers to submit a request to exercise their consumer rights.

Utah

The UCPA follows the same approach as Colorado, Connecticut, Iowa, and Virginia, providing that consumers have the right to confirm whether a controller is processing a consumer's personal data, and by requiring controllers to provide consumers with a reasonably accessible and clear privacy notice and inform them of:

- the categories of personal data processed by the controller;
- the purposes for which the categories of personal data are processed;
- how consumers may exercise their rights;
- the categories of personal data that the controller shares with third parties, if any; and
- the categories of third parties, if any, with whom the controller shares personal data.

Virginia

Virginia also follows the same approach as detailed above, with the exception of California, by providing that consumers must be informed, through the provision of a privacy notice, of:

- the categories of personal data processed by the controller;
- the purpose for processing personal data;
- how consumers may exercise their rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;
- the categories of personal data that the controller shares with third parties, if any;
- the categories of third parties, if any, with whom the controller shares personal data; and
- if a controller sells personal data to third parties or processes personal data for targeted advertising, to clearly and conspicuously disclose such processing, as well as the way a consumer may exercise the right to opt out of such processing.

USA Federal

The ADPPA establishes that covered entities must inform individuals of their processing activities when obtaining affirmative express consent, as well as in the form of a privacy policy as part of its transparency obligations.

When obtaining affirmative express consent for certain activities under the ADPPA, the request from the covered entity must be written in easy-to-understand language and specify:

- a description of the processing purpose for which the individual's consent is sought;
- the specific categories of covered data that the covered entity shall collect, process, and transfer necessary to effectuate the processing purpose;
- the individual's applicable rights related to consent; and
- the option to refuse consent, which must be at least as prominent as the option to accept, with the option to refuse taking the same or fewer number of steps as the option to accept.

Separately, covered entities must also make publicly available a privacy policy that provides a detailed and accurate representation of its data collection, processing, and transfer activities, including:

- the identity and contact information of the covered entity and any other entity within the same corporate structure to which covered data is transferred;
- the categories of covered data the covered entity collects or processes;
- the processing purposes for each category of covered data;
- whether the covered entity transfers covered data and, if so, each category of recipients, the name of each third-party collecting entity to which the covered entity transfers covered data, and the purposes for which such data is transferred;
- the length of time the covered entity intends to retain each category of covered data, including sensitive covered data or, if it is not possible to identify that timeframe, the criteria used;
- a prominent description of how an individual can exercise the rights described in the ADPPA;
- a general description of the covered entity's data security practices;
- the effective date of the privacy policy; and
- whether or not any covered data is transferred to, processed in, stored in, or otherwise accessible to the People's Republic of China, Russia, Iran, or North Korea.

5.2. Right of access

California
Uniquely, the CCPA as amended provides a general right to access as well as right to access associated with the sale and sharing of a consumer personal information. Specifically, consumers have the right to request that a business that collects a consumer's personal information disclose:

- the categories of personal information it has collected about that consumer;
- the categories of sources from which the personal information is collected;
- the business or commercial purpose for collecting, selling, or sharing personal information;
- the categories of third parties to whom the business discloses personal information; and
- the specific pieces of personal information it has collected about that consumer.

Regarding circumstances where a business sells or shares a consumers' personal information, a consumer has the right to request that a business disclose the following information:

- the categories of personal Information that the business collected about the consumer;
- the categories of personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal Information was sold or shared, by category or categories of personal information for each category of third-party parties to whom the personal information was sold or shared; and
- the categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom It was disclosed for a business purpose.

Colorado
The CPA provides a clearer right to access than the CCPA as amended, not differentiating access requirements based on type of processing. Specifically, the CPA provides consumers the right to confirm whether a controller is processing their personal data and to access their personal data.

Connecticut
Under Connecticut's CTDPA, the law continues to follow the approach of being limited in the wording of the right of access, but does provide consumers with the right to confirm whether or

not a controller is processing their personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret.

Iowa
Similar to other state laws, Iowa provides for the right of access.

Utah
Utah takes perhaps the least verbose angle, but nevertheless also affords consumers the right to access their personal data.

Virginia
Finally, Virginia does not deviate to the approaches in California, Colorado, Connecticut, and Utah, and also provides consumers with the right to confirm whether or not a controller is processing their personal data and to access such personal data (§59.1-577(A)(1) of the CDPA).

USA Federal
Under the ADPPA, upon receiving a verified request, covered entities must provide individuals with the right to access, in a human-readable format, their data that is collected, processed, or transferred within the 24 months preceding the request.

Individuals may also access information about, among other things, the third parties to whom their data has been transferred, the sources from which their data has been collected, and a description of the purpose for which their data has been transferred.

5.3. Right to rectification

California
The CCPA as amended provides a consumer the right to request a business that maintains inaccurate personal Information about the consumer correct such inaccurate personal Information, taking into account the nature of the personal Information and the purposes of the processing of the personal Information.

Additionally, a business must disclose to the consumer their right to request the correction of inaccurate personal information.

Colorado
Colorado's CPA, unlike the CCPA, expressly addresses consumers' right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of their personal data.

Connecticut
Similarly, the CTDPA not only takes the same approach as Colorado, but also follows the same wording in providing that a consumer has the right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of their personal data.

Iowa
Like in Utah, the ICDPA notably does not provide the right to correct personal data.

Utah
Contrastingly to the laws of California, Colorado, Connecticut, Iowa, and Virginia, the UCPA does not expressly refer to a right to rectify personal data.

Virginia
Finally, the CDPA follows the same provision and wording as Colorado and Connecticut in providing that consumers have the right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data.

USA Federal
Under the ADPPA, upon receiving a verified request, covered entities must provide individuals with the right to correct any verifiable substantial inaccuracy or substantially incomplete information. This includes the right to instruct the covered entity to make reasonable efforts to notify the corrected information to all third parties or service providers to which such data has been transferred.

5.4. Right to erasure

California
Under the CCPA as amended, a consumer has the right to request that a business delete any personal information about them which has been collected from the individual and businesses collecting such personal information must also disclose the consumer's right to request the deletion of their personal information to third parties. Moreover, the CCPA as amended further provides that a business may maintain a record of deletion requests for the purpose of preventing deleted data to be later processed or sold.

Colorado
The CPA takes a much more limited approach in addressing consumers' right to delete their personal data, by providing simply that consumers have such a right.

Connecticut
The CTDPA follows the approach of Colorado, as does Iowa, Utah and Virginia, by refraining from any extensive provisions, and instead simply noting that a consumer has the right to delete their personal data provided by, or obtained, about them.

Iowa
The ICDPA takes the same approach of Colorado, Connecticut, Utah and Virginia, providing the right to delete personal data provided by the consumer.

Utah
Likewise, the UCPA provides consumers with the right to delete their personal data.

Virginia
Finally, Virginia too follows in the trend seen between Colorado, Connecticut, Iowa, and Utah by simply providing that consumers have the right to delete personal data provided by, or obtained, about the consumer, thereby also following the wording as seen in Connecticut's CTDPA.

USA Federal
Under the ADPPA, upon receiving a verified request, covered entities must provide individuals with the right to delete their data. This includes the right to instruct the covered entity to make reasonable efforts to notify the individual's deletion request to all third parties or service providers to which such data has been transferred.

5.5. Right to object/opt-out

California

Under the CCPA as amended, consumers have an express right to opt-out, at any time, to the sale or sharing of personal information. In addition, consumers have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information.

Additionally, the CCPA as amended provides a further age restriction to the sale or sharing of personal information, noting that personal information of individuals over the age of 13 and under the age of 16 cannot be sold or shared, unless the consumer's parent or guardian, has affirmatively authorised the sale or sharing of the consumer's personal information. To this end, for minors the right to opt-out has been removed and requires express consent to continue with a sale or sharing (opt-in).

Furthermore, the right has an additional requirement with respect to third parties, in that the CCPA as amended requires a business selling consumers personal information to third parties to provide consumers with a notice that their information may be sold or shared and that they have the right to opt-out of such sale or sharing.

The CCPA as amended does not, however, address the right to withdraw consent.

Colorado

Here, the CPA, along with the laws of Connecticut, Utah, and Virginia, take a different approach to the right to opt-out as it is provided under California's CCPA as amended. Specifically, these other four state laws provide for the right to opt-out on a broader level that only to the sale or sharing of personal data.

As is concerns the CPA, a consumer has the right to opt out of the processing of personal data concerning them for purposes of:

- targeted advertising;
- the sale of personal data; or
- profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

One addition contained in the CPA is the express address of consumers' right to withdraw consent, as separate to any right to opt-out. In this respect, the CPA, in addressing the right to opt-out, notes that consumers may nevertheless consent to the processing of their data for targeted advertising or sale, but must be provided with a means to withdraw any such given consent.

Connecticut

The CTDPA takes the same approach and wording as seen in Colorado's CPA by providing that consumers have the right to opt of the processing of their personal data for purposes of:

- targeted advertising;
- the sale of personal data; or
- profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Like California, Utah, and Virginia, and unlike Colorado, the CTDPA does not expressly address a right to withdraw consent.

Iowa

The IDCPA also includes the right to opt-out of the sale of personal information.

Unlike Colorado, Connecticut, Virginia, and Utah, Iowa's consumer opt-out rights do not apply to pseudonymous data where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to appropriate technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

While there is no explicit right to opt-out of targeted advertising in the ICDPA's consumer rights section, there is a requirement for controllers that engage in targeted advertising provide clear and conspicuous disclosure as a means to opt out.

Similar to the CCPA as amended, the ICDPA does not address the right to withdraw consent.

Utah
The UCPA slightly deviates from the approaches in Colorado, Connecticut, and Virginia by excluding profiling as a basis for the right to opt out, but nevertheless provides that consumers have the right to opt out of the processing of their personal data for:

- targeted advertising; or
- the sale of personal data.

Like California, Connecticut, and Virginia, and unlike Colorado, the UCPA does not expressly address a right to withdraw consent.

Virginia
Finally, Virginia mirrors the approaches in Colorado and Connecticut by providing consumers with the right to opt out of the processing of their personal data for purposes of:

- targeted advertising;
- the sale of personal data; or
- profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

The CDPA also does not explicitly refer to the possibility of withdrawing consent.

USA Federal
The ADPPA provides two opt-out rights, namely the right to opt out of data transfers and the right to opt out of targeted advertising.

Notably, unlike the state laws, the right to opt of data transfers under the ADPPA is not explicitly limited to the sale of personal data, but instead includes all means to disclose, release, disseminate, make available, license, rent, or share covered data orally, in writing, electronically, or by any other means. Nevertheless, covered entities may refuse such right where the transfer is carried out on the basis of a permissible purpose under §101(b)(1) to (15) of the ADDPA.

Separately, the ADPPA requires covered entities to provide individuals with clear, conspicuous, and easy-to-execute means to withdraw any affirmative express consent previously provided.

5.6. Automated decision-making

California
The CCPA as amended does not explicitly refer to the right not to be subject to automated decision-making. However, the CCPA as amended stipulates that the CPPA may adopt regulations in areas

which include the governing of access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.

Colorado
While the CPA does not expressly and separately address the right not to be subject to automated decision-making, it couples considerations around such a requirement with consumers' right to opt out of, among other things, the processing of personal data concerning them for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects.

Connecticut
Similarly, the CTDPA also addresses automated decision-making indirectly through consumers' right to opt of certain processing, but providing them with a right to opt-out of processing for purposes of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning them.

Iowa
In line with Utah, the IDCPA notably does not provide the right to not be subject to fully automated decisions.

Utah
Like Iowa, the UCPA does not expressly provide for a right not to be subject to automated decision-making, nor does it address this indirectly.

Virginia
Finally, and as we have seen in Colorado and Connecticut, the CDPA indirectly addresses automated decision-making by providing that consumers have the right to opt out of the processing of their personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning them.

USA Federal
Although there are no explicit rights for individuals to object to automated-decision making, the ADPPA does provide for the right to opt-out of targeted advertising (see §204(c) of the ADPPA).

The ADPPA also confers certain civil rights protections, particularly in relation to discrimination and algorithms. Accordingly, covered entities may not collect, process, or transfer data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, colour, religion, national origin, sex, or disability, except under limited circumstances. Covered entities are also expected to conduct impact assessments and evaluations for covered algorithms.

5.7. Data portability

California
The CCPA as amended does not explicitly provide for the right to data portability. However, as part of the notice, disclosure, correction, and deletion requirements, it establishes that businesses shall provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hinderance.

Colorado
The CPA also expressly addresses consumers' right to data portability by providing that when exercising the right to access personal data, a consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows them to transmit the data to another entity without hinderance. A consumer may exercise this right no more than two times per calendar year.

Connecticut
The CTDPA takes the same approach as Colorado, Utah, and Virginia, with the same and comparable wording to the EU approach being adopted, and provides that consumers have the right to obtain a copy of their personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hinderance, where the processing is carried out by automated means, provided such controller will not be required to reveal any trade secret.

Iowa
Meanwhile, the ICDPA provides that consumers have the right to obtain a copy of the consumer's personal data, except as to personal data defined as 'personal information' under the §715C.1 *et seq*. of Title XVI of the Iowa Code that is subject to a security breach protection, that the consumer previously provided to the controller in a portable, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hinderance, where the processing is carried out by automated means.

Utah
Likewise, the UCPA notes that consumers have the right to obtain a copy of their personal data in a format that, to the extent that it is technically feasible, is portable; to the extent that it is practicable, is readily usable; and which allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.

Virginia
Finally, and likewise, the CDPA also provides that consumers have the right to obtain a copy of their personal data that they previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hinderance, where the processing is carried out by automated means.

USA Federal
The ADPPA provides that, upon receiving a verified request, covered entities must provide individuals with the right, to the extent technically feasible, to export their data to the individual or directly to another entity. This includes inferences linked or reasonably linkable to the individual but not derived data. In this regard, the data must be exported in a human-readable format that a reasonable individual can understand and download from the Internet, as well as in a portable, structured, interoperable, and machine-readable format.

6. Enforcement

As a general rule, State Attorneys General are the regulators for the comprehensive privacy laws in Colorado, Connecticut, Iowa, Utah, and Virginia, with only California having a dedicated authority established for this purpose. The role these regulators have is similar across all six laws including powers in relation to issuing regulations and rules, investigating violations, and taking enforcement actions. However, one difference seen between the six laws is with respect to the possibility of cure periods for violations. Utah and Virginia provide a 30-day cure period, whereas, Colorado and Connecticut offer a 60-day cure period, and Iowa provides for a 90-day cure period.

Monetary penalties that can be sought for violations of each of the six comprehensive privacy laws do, however, present some variety. One of the first notably differences is that Colorado and Connecticut do not expressly provide for set penalties, but instead apply penalties applicable to unfair or deceptive trade practices, as violations of their laws. Colorado and Connecticut also provide a very different penalty amount in this respect, with the former providing for penalties of not more than $20,000 per violation, and the latter calling for not more than $5,000 per violation. Contrastingly, California, Iowa, Utah, and Virginia adopt the same approach in providing for penalty amounts within their laws directly, although California provides a penalty range of $2,500 per violation or $7,500 for each intentional violation, while Iowa, Utah and Virginia simply note a penalty of not more than $7,500 per violation.

Civil remedies are one of the most debated topics within the discussions of comprehensive state privacy laws, specifically on whether a law is to allow or not a private right of action for individuals. In this regard, the six laws show complete unity in not providing for individuals' private right of action for any violations of the laws.

The ADPPA calls for the creation of a Bureau of Privacy within the FTC and is enforceable by the FTC, state attorneys general or privacy authorities, and private citizens, although private rights of action are prohibited within the first two years following enactment. Unlike with the abovementioned six laws, the ADPPA does not contain specific monetary penalties for non-compliant entities.

As such, here too we can see some differences between the six state privacy laws and the ADPPA. Therefore, this section addresses the similarities and differences with respect to supervisory authorities and powers, monetary penalties, and civil remedies.

Please note that further information may be provided in supplementary regulations or guidance issued by regulatory bodies.

6.1. Supervisory authorities

California

The CCPA as amended is enforced by the CPPA, who is responsible for initiating investigations and, where a business has been held to be in violation of a provision under the CCPA as amended, has the power to bring an enforcement action. Moreover, the CCPA as amended allows the CPPA to adopt regulations on various topics relevant to the provisions of the CCPA as amended, including, but not limited to updating or amending definitions, establishing certain exceptions as well as certain rules and procedures.

Colorado

Unlike California, which has a dedicated authority to regulate and enforce the comprehensive state privacy law, the CPA is enforced by the Colorado AG. In particular, the CPA provides the AG and/or District Attorneys with the power to enforce the CPA. However, and before taking any action for a violation, the AG or District Attorneys are required to issue a notice of violation to the controller if a cure is possible, and to allow for such a cure. If, however, a controller fails to cure a violation within a period of 60 days after having received the notice, an action may be brought against them. Notably, this provisions under the CPA would be repealed from 1 January 2025.

Moreover, and similarly to California, the CPA notes that the rules may be promulgated in furtherance of the CPA's provisions, with this being done by the AG. More specifically, such rules would focus on establishing one or more universal opt-out mechanisms, with any such rules needing to be established by 1 July 2023. The CPA addresses the possibility of additional rules and measures, with various deadlines by which these may be expected, covering topics such as rules around the process of issuing opinion letters and interpretive guidance to develop an operational framework for business that includes a good faith reliance defence of an action that may otherwise constitute a violation.

Connecticut

Like in Colorado, Iowa, Utah, and Virginia, where there is no designated regulatory authority, the Connecticut AG is responsible for enforcing the CTDPA. In particular, and during the period beginning on 1 July 2023 and ending on 31 December 2024, the AG must issue a notice of violation to the controller if the AG determines that a cure is possible, and must do so before initiating any action for a violation of the CTDPA. If the controller fails to cure their violation within 60 days of receipt of the notice, the AG may bring an action against them.

Furthermore, and no later than 1 February 2024, the AG is required to submit a report to the joint standing committee of the Connecticut General Assembly, disclosing:

- the number of notices of violation issued;
- the nature of each violation;
- the number of violations that were cured during the 60-day cure period; and
- any other matter the AG deems relevant .

Iowa

Similar to laws in Colorado, Connecticut, Utah and Virginia, the ICDPA is enforced by the Iowa AG. In particular, the AG will provide a written notice to the controller or processor identifying the specific violations of the ICPDA prior to initiating any enforcement actions. Interestingly, the cure period under the ICDPA is 90 days from the receipt of the AG notice, thus making it the longest among the six laws. If the violation is not cured within this period, an action may be brought by the AG.

Utah

Utah's UCPA is also regulated and enforced by the Utah AG, as in Colorado, Connecticut, Iowa, and Virginia, although the UCPA additionally provides the Division of Consumer Protection within the Utah Department of Commerce with certain assistance powers to the AG, particularly with respect to investigations.

Specifically, and upon referral from the Division of Consumer Protection, the AG may initiate an enforcement action against a violating controller or processor, but must provide written notice identifying the violations alleged, and an explanation of the basis for each allegation at least 30 days before initiating an enforcement action, and must allow for a cure period of 30 days, only after which enforcement may be sought. In this regard, the UCPA differs to Colorado and Connecticut, but compares to California and Virginia, in providing for a 30-day cure period instead of 60 days.

As it concerns the Division of Consumer Protection, it is afforded investigative powers under the UCPA, and must establish and administer a system to receive consumer complaints regarding a controller's or processor's alleged violation of the UCPA. Additionally, it may investigate consumer complaints to determine whether a violation has occurred, and if it determines that there is reasonable cause to believe that substantial evidence exists for a violation of the UCPA, the matter should be referred to the AG. The Division of Consumer Protection is also authorised to, upon request, provide consultation and assistance to the AG in enforcing the UCPA.

Virginia

Like Colorado, Connecticut, Iowa, and Utah, Virginia's CDPA is regulated and enforced by the Virginia AG, who also has investigative powers. However, and similarly to the other five state privacy laws, before an action for a violation is initiated, the AG is required to provide the violating controller or processor with a notice, which must be sent 30-days before initiating any action, and thereby allowing the violator a 30-day cure period. If the violation is not cured within this period, an action may be brought by the AG.

USA Federal

The FTC has been designated as the federal authority responsible for ensuring compliance with the ADPPA and issuing mandated guidelines, although a newly-established Bureau of Privacy will be tasking with assisting the FTC in carrying out the duties under the ADPPA. It must be staffed and fully operational not later than one year after the ADPPA comes into force.

On a state-level, the ADPPA allows the attorney general or state privacy authority to bring civil action in the name of the state, which would then be brought exclusively in an appropriate Federal district court.

6.2. Monetary penalties

California

The CCPA as amended establishes civil penalties in cases of non-compliance with its provisions. Specifically, a business, service providers, or contractors failing to rectify an alleged violation within the provided cure period will be held to be in violation of the CCPA as amended, subject to an injunction, and liable for a civil penalty of not more than $2,500 per violation or $7,500 for each intentional violation.

Colorado

Although the CPA, unlike California, does not expressly outline monetary penalties for violations of its provisions, it provides that any violation of the CPA is considered a deceptive trade practice, which carries certain penalties. Specifically, and generally, violations will be subject to a civil penalty of not more than $20,000 for each violation, with other penalties applied for certain other violations, such as against an elderly person or against a court order or injunction.

Additionally, and as further contrast to California, this penalty is provided as a maximum, although lesser penalties may also be imposed, while California offers set penalty amounts for violations.

Connecticut

Similarly, Connecticut's CTDPA also does not expressly provide for monetary penalties, but instead notes that a violation will be deemed an unfair trade practice, and therefore subject to penalties under that applicable statute. Specifically, Connecticut's laws in this regard note that if it is found that a person committed an unfair trade practice, a civil penalty of not more than $5,000 for each violation may be sought.

Iowa
In line with Utah and Virginia, the ICDPA expressly states the civil penalty amount that may be sought for violations. Specifically, the ICDPA provides that the AG may seek an injunction to restrain any violations, and civil penalties of up to $7,500 for each violation.

Utah
Contrastingly to Colorado and Connecticut, the UCPA follows the approach of California by directly noting the civil penalty amount that may be sought for violations. Specifically, the UCPA provides that the AG may recover actual damages to the consumer, and for each violation an amount not to exceed $7,500.

Virginia
Finally, Virginia also deviates from the approaches by Colorado and Connecticut in referring to violations in the context of unfair or deceptive trade practices, and instead directly provides for the penalties that may be imposed for violations of the CDPA. As such, the CDPA the AG may initiate an action for violations and may seek an injunction to restrain any violations, and civil penalties of up to $7,500 for each violation.

USA Federal
The ADPPA does not explicitly address the issuance of administrative monetary penalties. However, the ADPPA provides that the FTC will enforce the ADPPA and the regulations promulgated thereunder in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the FTC Act.

However, monetary compensation, relief, and damages are discussed in the context of civil action and the Privacy and Security Victims Relief Fund. For instance, persons may receive an amount equal to the sum of any compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs.

6.3. Civil remedies for individuals, including other remedies

California
While the CCPA as amended provides for a civil remedy in relation to data security breaches, where consumers may individually seek relief where their non-encrypted or non-redacted personal information is subject to unauthorised access and exfiltration, theft, or disclosure because of the business' violation of security obligations, it does not expressly address civil remedies or a private right of action with respect to the overall provisions of the CCPA as amended. In fact, the CCPA as amended provides that a cause of action shall apply only to violations with respect to data breaches and will not be based on violations of any other provisions of the CCPA as amended, where nothing can be interpreted to serve as the basis for a private right of action under any other law.

Colorado
Colorado's CPA takes the same approach as the other five privacy laws, and does not authorise a private right of action for violations of its provisions.

Connecticut
Likewise, the CTDPA also provides that nothing in its provisions shall be construed as providing the basis for, or be subject to, a private right of action for violations.

Iowa
The ICDPA adopts the same approach as the other five privacy laws and provides that nothing in the ICDPA shall be construed as providing the basis for, or be subject to, a private right of action for violations.

Utah
Similarly, Utah's UCPA also does not establish a private right of action, both under the UCPA itself and under any other law.

Virginia
Finally, Virginia also follows the approaches in California, Colorado, Connecticut, Iowa, and Utah in not noting that there is no basis for a private right of action for violations of its provisions or under any other law.

USA Federal
The ADPPA explicitly provides for various civil rights and algorithms, as well as conditions for enforcement by persons. Persons may receive an amount equal to the sum of any compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs.

Any person or class of persons may bring a civil action against a covered entity or service provider in any Federal court of competent jurisdiction.

In addition, the ADPPA calls for a 'Privacy and Security Victims Relief Fund' in the Treasury of the US, so that, in any judicial or administrative action under the ADPPA or its regulations, the amount of any civil penalty obtained against a covered entity or service provider, or any other monetary relief ordered to be paid to provide redress, payment, compensation or alike, but where the impacted individuals cannot be located, should be deposited into the fund.

Report

Comparing Privacy Laws:

OneTrust DataGuidance's benchmark report comparing the GDPR against both the CCPA and CPRA provides information for businesses on the differences and similarities between these three laws. Its comparisons on scope of application, legal basis, controller and processor obligations, data subject rights, and enforcement can be leveraged to better understand the requirements under each law in order to facilitate compliance efforts.

Download Report

The full report can be found online at www.dataguidance.com

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE