

Data Privacy Laws in the US States

Explore Data Privacy
Laws from Coast to Coast

Table of Contents

Introduction

California Privacy Rights Act

What is CPRA?	3
What is the Purpose of CPRA?	3
What is CPPA?	3
New Regulations in the CPRA	4
How CPRA Affects an Organization's Data Privacy Policy	7
Here are Commonly Asked Questions Related to the CPRA	8

Colorado Privacy Act

Colorado Privacy Act (CPA)	12
What is the Colorado Privacy Act?	12
Who Needs to Comply with CPA?	12
Obligations for Organizations Under CPA	13
Data Subject Rights Under CPA	14
Regulatory Authority	16
Any Important Exemptions	16
Penalties for Non-Compliance	17
How an Organization Can Operationalize the CPA	17

Connecticut Data Privacy Act

What is CTDPA?	19
Who Needs to Comply With the CTDPA	19
Obligations for Organizations Under the CTDPA	21
Data Subject Rights Under CTDPA	24
Regulatory Authority	26
Any Important Exemptions	27

Penalties For Non-Compliance	28
How an Organization Can Operationalize the CTDPA	28

Delaware Personal Data Privacy Act

What is DPDPA?	30
Who Needs to Comply with DPDPA	30
Obligations for Organizations Under DPDPA	32
Data Subject Rights	37
Regulatory Authority	39
Limitations	39
Penalties for Non-Compliance	41
How an Organization Can Operationalize DPDPA	42

Florida Digital Bill of Rights

What is the Florida Digital Bill of Rights?	44
Who Needs to Comply with the FDBR	44
Obligations for Organizations Under FDBR	47
Data Subject Rights Under FDBR	52
Regulatory Authority	54
Limitations	54
Penalties for Non-Compliance	56
How an Organization Can Operationalize the FDBR	57

Indiana's Consumer Data Protection Act

What is ICDPA?	59
Who Needs to Comply with the ICDPA	59
Obligations for Organizations Under ICDPA	61
Data Subject Rights	64
Regulatory Authority	66
Limitations	67
Penalties For Non-Compliance	69
How an Organization Can Operationalize ICDPA	69

Iowa's Data Privacy Law

What is Iowa's Data Privacy Law - Senate File 262?	71
Who Needs to Comply with the Law	71
Obligations for Organizations Under the Law	72
Data Subject Rights	74
Regulatory Authority	76
Any Important Exemptions	76
Limitations	77
Penalties for Non-Compliance	78
How an Organization Can Operationalize the Law	79

Montana's Consumer Data Privacy Act

What is MCDPA?	81
Who Needs to Comply with the MCDPA	81
Obligations for Organizations Under MCDPA	83
Data Subject Rights	86
Limitations	88
Regulatory Authority	90
How an Organization Can Operationalize the MCDPA	90

Oregon's Consumer Privacy Act

What is OCPA (Senate Bill 619)?	92
Who Needs to Comply with OCPA	92
Obligations for Organizations Under OCPA	94
Data Subject Rights	99
Regulatory Authority	102
Limitations	102
Penalties for Non-Compliance	103
How an Organization Can Operationalize the OCPA	103

Texas Data Privacy and Security Act

What is TDPSA?	105
----------------	-----

Who Needs to Comply with TDPSA	105
Obligations for Organizations Under TDPSA	107
Data Subject Rights	111
Regulatory Authority	113
Limitations	114
Penalties for Non-Compliance	115
How an Organization Can Operationalize the TDPSA	115

Tennessee Information Protection Act

What is TIPA?	118
Who Needs to Comply with the Law	118
Obligations for Organizations Under the TIPA	120
Data Subject Rights	125
Regulatory Authority	127
Limitations	127
Penalties for Non-Compliance	129
How an Organization Can Operationalize TIPA	129

Utah's Consumer Privacy Act

What is UCPA?	132
Who Needs to Comply with the Law?	132
Obligations for Organizations Under UCPA	134
Data Subject Rights Fulfillment	136
Regulatory Authority	138
Limitations	138
Penalties for Non-Compliance	139
How an Organization Can Operationalize the UCPA	139

Virginia Consumer Data Protection Act

What is VCDPA?	142
Who Needs to Comply with VCDPA?	142

Obligations for Organizations Under VCDPA	143
Data Subject Rights	144
Regulatory Authority	146
Any Important Exemptions	146
Penalties for Non-Compliance	147
How Organizations Can Operationalize VCDPA	147

[Meet Global Data Compliance with Securiti PrivacyOps](#)

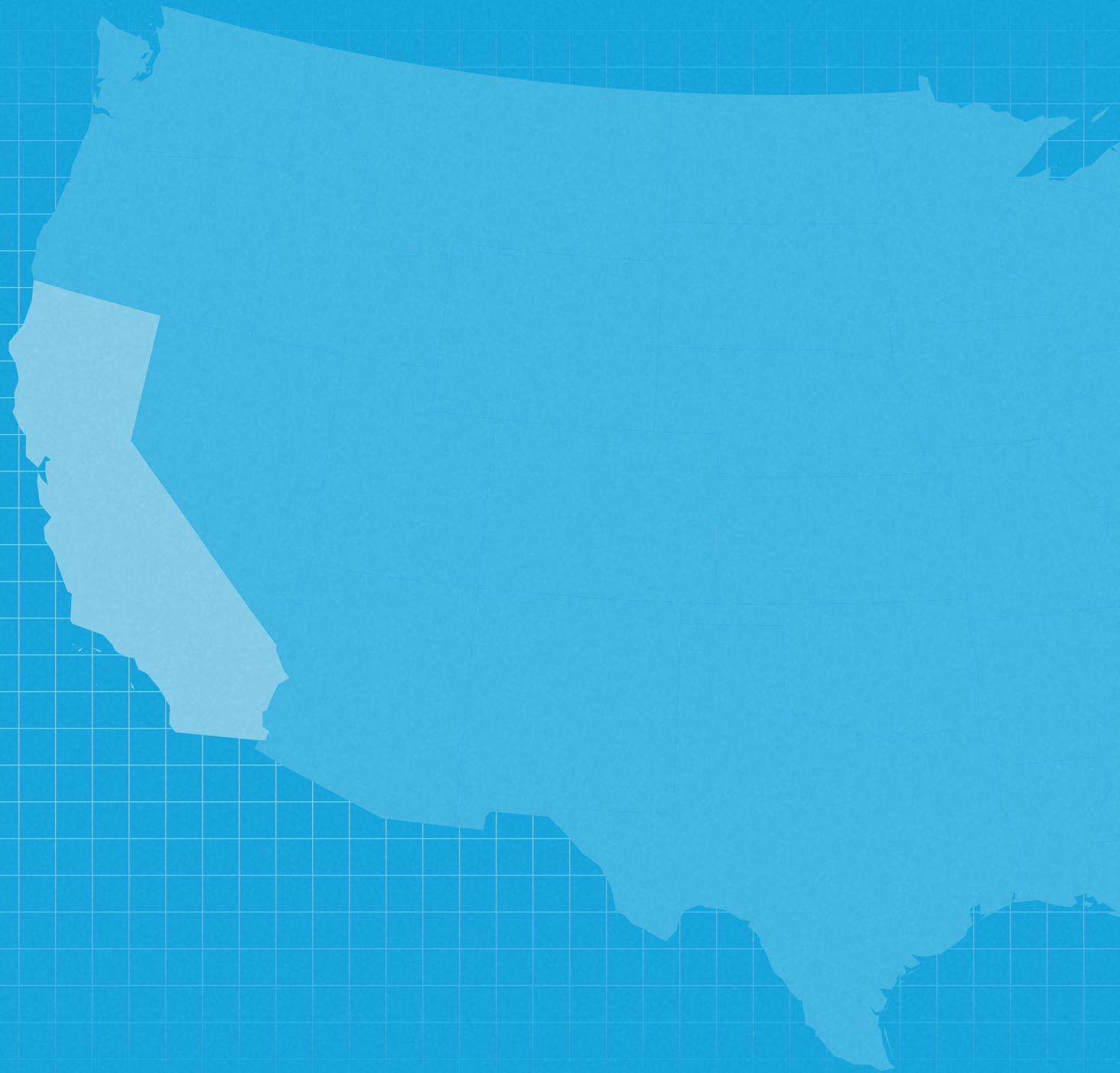
Introduction

Data privacy has been a fairly complex topic within the United States of America. Unlike the EU or other major Western economies, the US does not have a comprehensive federal data privacy regulation that provides adequate privacy protection to its citizens. While there has been some progress, with a potential draft presented in the House and President Biden emphasizing the need for better data privacy in his latest State of The Union Address, a GDPR-like regulation within the US remains elusive.

Amidst all this, the states have taken it upon themselves to protect their citizens' digital data privacy rights. Since California passed its landmark CCPA, several other states have followed suit.

This whitepaper is put together to offer a comprehensive guide to the existing and upcoming data privacy laws in the United States. By explaining the state-level privacy laws, the whitepaper intends to help organizations, privacy professionals, and legal teams better understand the laws for informed decision-making and compliance.

California Privacy Rights Act



What is CPRA?

The California Privacy Rights Act (CPRA) is California's state legislation that protects its residents' digital privacy. It went into effect on January 1, 2023, and mandates all businesses to audit their data collection, storage, processing, and sharing mechanisms to ensure they are in compliance with the law.

The CPRA builds on earlier legislation known as the California Consumers Privacy Act (CCPA), which came into effect on January 1, 2020. The CPRA will be enforced by the first dedicated data protection authority in the United States: the California Privacy Protection Agency (CPPA).

What is the Purpose of CPRA?

When the General Data Protection Regulation (GDPR) came into effect in 2018, it was meant to ensure that any organization dealing with the personal data collected within the EU would have to make concrete efforts to protect it and the privacy of the data subjects whom it concerns. It didn't matter if the organization operated from inside the EU or based elsewhere as it applied to any company that dealt with the personal data of data subjects who were residents of the EU.

The California Privacy Rights Act (CPRA) is similar in its scope as it applies to 'for profit' entities dealing with the personal information of California residents, which meets one of three criteria. The three criteria for a business to fall under the CPRA's jurisdiction are:

Firstly, businesses that share the personal information (PI) of at least 100,000 consumers or households will be subject to the CPRA. This is an update on the CCPA's earlier threshold of 50,000 consumers, making it a friendlier piece of legislation for small-to-medium enterprises.

Secondly, a business that makes \$25 million in gross revenue by January 1 of the preceding year will also be subject to the California Privacy Rights Act regulations.

Lastly, businesses that receive 50% or more of their gross revenues from sharing or selling personal information collected on users also come under CPRA's jurisdiction.

What is CPPA?

After the CPRA was passed, it established the California Privacy Protection Agency (CPPA) as the primary body responsible for safeguarding all Californian's digital privacy. The CPRA gives the CPPA full legal, administrative, and enforcement rights regarding matters related to the CPRA. The CPPA's board comprises five members, in addition to a chairperson and an executive director.

The CPPA has four primary responsibilities in relation to the CPRA: education, rulemaking, enforcement,

and certifications. The CPPA has an annual budget of \$10 million to aid it in its efforts to carry out these responsibilities.

The CPPA has the power to certify businesses that are CPRA-compliant. This certification can be used by businesses and entities that do not have to conform to CPRA regulations but want to voluntarily illustrate that their data protection practices are of the highest standards possible.

Moreover, considering California is one of the most lucrative business locations in the world, companies might find that a CPPA certification gives them an additional competitive edge in a more privacy-aware consumer market.

New Regulations in the CPRA

The California Privacy Rights Act (CPRA) introduced new requirements related to the protection and management of the personal information of consumers. Here's what you should know:

CPRA Creates a New Category of Sensitive Personal Information (SPI)

The CPRA creates a new category of personal information called Sensitive Personal Information (SPI), which is subject to stricter disclosure and purpose limitation requirements. Since the CPRA also specifies that security measures for data must be appropriate for the data type, it would be reasonable to assume that SPI would require additional safeguards and protections.

Most importantly, the CPRA allows customers to request that businesses limit the usage of consumers' SPI. SPI contains very sensitive information sets such as:

- Social Security Number;
- Driver's license;
- State identification card;
- Passport Number;
- Financial account information and log-in credentials;
- Debit Card or Credit Card number along with access codes;
- Precise geolocation data;

- Religious or philosophical beliefs;
- Ethnic origin;
- Contents of communication;
- Genetic data;
- Biometric information for identification;
- Health information;
- Information about sex or sexual orientation.

CPRA Demands New Links on a Website

The CPRA revises the standards for how a website enables users to exercise their right to limit the use of their SPI and adds a requirement for how a website enables users to opt out of having their PI sold or shared.

The CPRA modifies the CCPA's Do Not Sell button, requiring a website to have a link that says "Do Not Sell Or Share My Personal Information."

The CPRA also adds a new obligation for a website to have a link labeled "Limit The Use Of My Sensitive Personal Information," enabling Californians to control how their SPI is used and disclosed.

Furthermore, the CPRA recommends enterprises create "a single, clearly labeled link" that allows consumers to opt-out of the sale or sharing of PI while also limiting the use or disclosure of their SPI.

CPRA Creates New DSR Requests and Amends Existing CCPA Rights



Right to correction

Consumers have the right to request that their PI and SPI be changed if they discover that it is incorrect.



Right to opt-out of automated decision-making

Californians can refuse to have their PI, and SPI used to make automated conclusions, such as profiling for targeted behavioral advertising.



Right to know about automated decision-making

Californians can ask for information on how automated decision technologies work and their likely outcomes.



Right to limit the use of sensitive personal information

Californians can compel corporations to limit the use of special categories of personal data, particularly when it comes to third-party sharing.



Right to Delete

Consumers can now request that businesses direct third-party suppliers, service providers, or contractors to erase personal information that the company may have sold or shared with them.



Right to Access

Businesses are now required to also report all PI data they have shared with third parties and the third parties with whom they have shared the PI.



Right to Opt-Out

Data subjects can opt out of having their personal information sold or shared with third parties, including for cross-context behavioral advertising.



Right to Data Portability

Data subjects can request that organizations send certain pieces of personal information to another entity. This transmission, however, must be technically feasible for the company.



Right of Minors

Businesses must now notify minors if they intend to sell or share their personal information. It's also worth noting that if a consumer under the age of 16 refuses to give their approval for a business to sell or share their personal information, the business must either wait another 12 months or wait until the consumer becomes 16 before asking for their opt-in consent again.

CPRA Governs Behavioral Advertising

The California Privacy Rights Act (CPRA) modifies the CCPA to govern behavioral advertising that uses personal information to profile California citizens and promote advertisements.

CPRA introduces the California Privacy Protection Agency (CPPA)

As mentioned before, the California Privacy Protection Agency (CPPA) is designated as the principal enforcer and supervisor of the CPRA data privacy regime. It is the first dedicated data protection authority created within the USA.

CPRA takes inspiration from the EU's GDPR

CPRA adds GDPR-like provisions to the CCPA, such as data minimization and retention requirements, as long as mandating businesses that undertake 'risky processing' to conduct and publish risk assessments.

How CPRA Affects an Organization's Data Privacy Policy

Collection Notice

Under the CCPA, websites are required to ensure consumers know exactly when their data is being collected. However, under the California Privacy Rights Act (CPRA), organizations must go into additional detail about how and why they need to collect a user's data. The three main additional notices include the responsibility to disclose if the organizations share their personal information (PI), collect any of their sensitive personal information (SPI), and how long they retain the data being collected.

Privacy Policy

It is natural that the new CPRA regulation requires companies to alter their existing privacy policies. The most notable changes include letting the user know if they plan to "share" their data in addition to "selling" their data. Under the CCPA, companies only needed to let users know if they planned on selling their data.

Rights of Customers Under CPRA

The new CPRA guarantees all residents in California certain rights. It is the responsibility of all businesses that fall under the CPRA's jurisdiction to ensure these rights are fulfilled. An exhaustive list of CPRA rights includes:

- Right to Delete Personal Information
- Right to Correct Inaccurate Personal Information
- Right to Know What Personal Information is Being Collected
- Right to Access Personal Information
- Right to Know What Personal Information is Sold or Shared and to Whom
- Right to Opt-Out of Sale or Sharing of Personal Information
- Right to Limit Use and Disclosure of Sensitive Personal Information

Here are Commonly Asked Questions Related to the CPRA



How does the CPRA change privacy laws in California, and am I impacted?

Any business with \$25 million annual gross revenue in the previous calendar year or buys/sells/shares personal information of 100,000 consumers or households or derives 50% or more of its revenue from selling/sharing personal information is obliged to CPRA compliance.

Besides that, the CCPA's exception for employee personal information has ended, and businesses must implement a CPRA compliance program that includes their employees' information. Other major changes include the requirement to respect a consumer's opt-out preference signal, such as the GPC and expand the "Do Not Sell" opt-out requirement to "Do Not Sell or Share" as well as revising their current vendor contracts to ensure they fulfill the requirements laid down in the CPRA for such arrangements.



What is sensitive personal information under the CPRA?

Under the CPRA, sensitive personal information is any information that reveals a consumer's personal identification numbers such as social security number, driver's license, passport, state ID, credit/debit card numbers as well as relevant passwords, geolocation, racial origin, sexual orientation, union membership, religious or political beliefs, as well as the consumer's biometric data.



What new rights does the CPRA give consumers?

One of the most important changes the CPRA brings compared to the CCPA is the consumers' right to correct information collected on them by organizations online. This can include any information that may have become inaccurate, incomplete, or obsolete since it was collected.



What is the purpose limitation under the CPRA?

The purpose limitation introduced by the CPRA is, at its core, a lot like the data minimization of the GDPR. Purpose limitation requires organizations collecting users' information to have a specific and explicit reason for doing so.



What does CPRA say about minors' personal information?

Much like the CCPA, the CPRA ensures that organizations cannot sell or share a child's personal information unless the child (at least 13 years old) or the child's parents (less than 13 years old) explicitly authorize the selling or sharing of such information. If, in such cases, consent is not

provided, then the organization must wait at least 12 months before requesting consent again or wait until the child turns 16.

However, these obligations apply only if the organization has “actual knowledge” of the child’s age. In any case, the organization must comply with all its relevant obligations under the federal Children’s Online Privacy Protection Act (COPPA) regarding the personal information of children under the age of 13.



Who enforces the CPRA?

The CPRA is enforced primarily by the newly created California Privacy Protection Agency (CPPA).



What notice obligations does the CPRA introduce?

Presently, the CCPA requires businesses to inform users of all categories of personal information to be collected and the purpose behind their collection. The CPRA expands these requirements with the organizations collecting the data now required to inform the users if their data will be sold or shared, how long their data will be retained, and more detailed information related to the collection of sensitive personal information.



Does the CPRA introduce a new applicability scope?

The CPRA expands the applicability scope under the CCPA by altering the definition of “businesses”. There are four categories under the CPRA. Directors of Processing, Common Branding, Joint Ventures, and Certified Businesses.



What CCPA exceptions are impacted by the CPRA?

The CPRA introduces several modifications, clarifications, and changes to the exceptions made in the CCPA. These include the Trade Secret Exemption, Household Data Exemption, Student Information and Assessments Exemption, Physical Item Exemption, Commercial Credit Reporting Agency Exemption, Public Information Exemption, De-Identified Information Exemption, Fair Credit Reporting Act Information Exemption, Car Dealer-Manufacturer Exemption, Financial Information Exemption, Aggregate Information Exemption, Medical Information Exemption, Healthcare Providers and Covered Entities Exemption, Clinical Trial Exemption, Driver’s Privacy Protection Act of 1994 Exemption, Evidentiary Privilege Exemption, and Legal Compliance and Law Enforcement Cooperation Exemption.



Does the CPRA introduce any security assessment requirements?

Yes, the CPRA introduces a new information security auditing requirement for businesses that requires an annual cybersecurity audit of companies that process personal information that poses a significant risk to consumers’ privacy. The results of such assessments must be provided to the CPPA to ensure an organization complies with its security responsibilities per the CPRA guidelines.



Does CPRA apply to non-profit organizations and government agencies?

Similar to CCPA, the CPRA only applies to “for-profit” organizations. This further means that the CPRA provisions do not apply to government agencies or non-profit organizations.



What violations does CPRA impose?

California Privacy Rights Act (CPRA) has outlined fines with regard to violations in section 1798.155, Administrative Enforcement. The legislation states that any covered businesses, service providers, or contractors that violate CPRA provisions will be fined up to \$2,500 for each violation. However, when it comes to the violation of the personal information of minors, CPRA increases the fine to up to \$7,500 for each intentional violation.

The legislation further clarifies that the money received from the administrative fine and settlements will be deposited to the Consumer Privacy Fund. These funds will then be used to counterbalance the costs incurred by the regulatory authority (CPPA), state court, or any attorney general.



What is the CPRA look-back period?

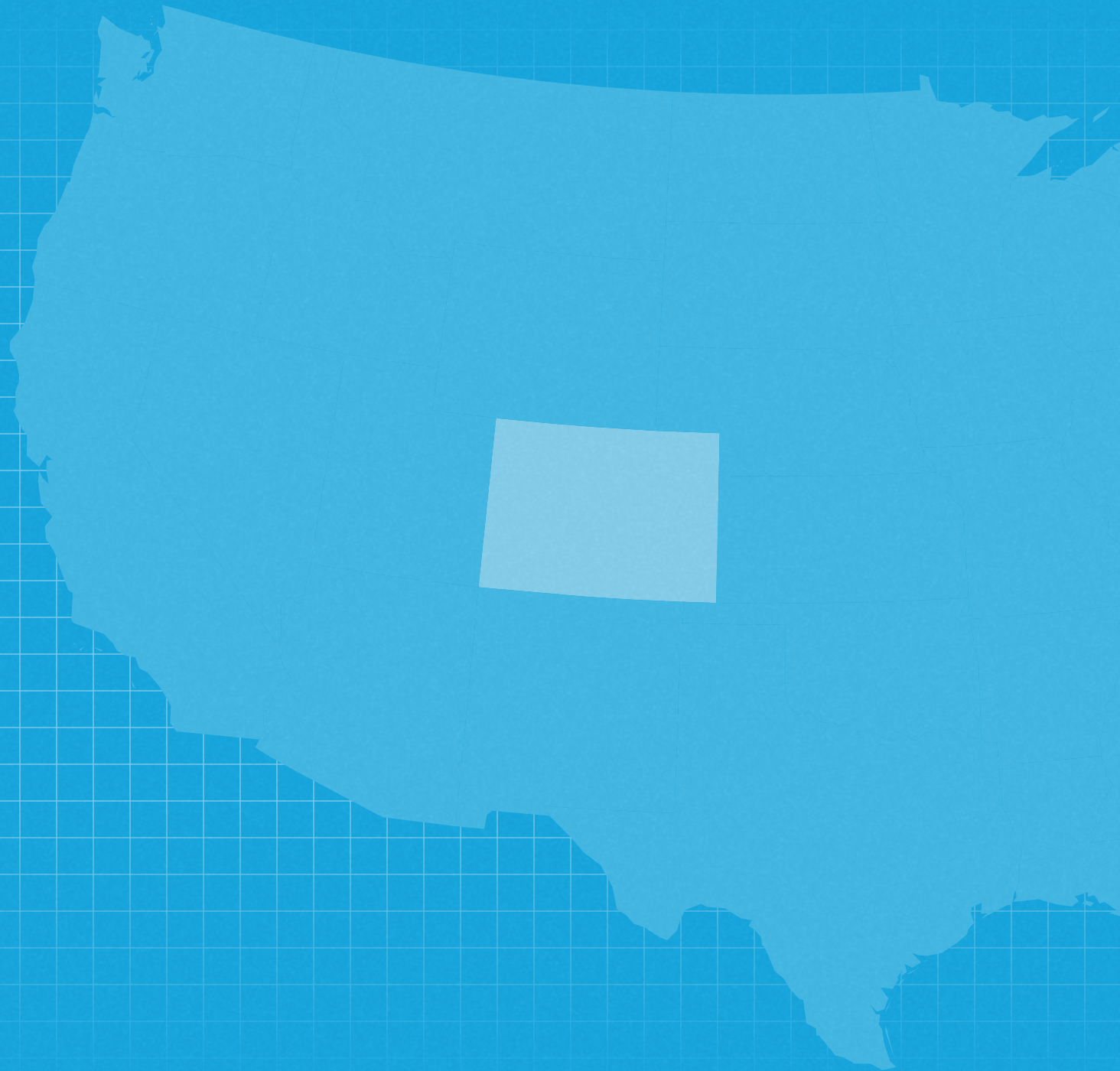
Businesses shouldn't assume that the changes brought by CPRA will be effective from January 1, 2023. Indeed, it will be effective from 2023, but it is not as straight as an arrow. The CPRA introduces a rather sneaky provision, i.e., the “look back” period. The provision enables consumers to request access to their data that even goes back to January 1, 2022. This means that some exemptions that were provided in the CCPA but removed in the CPRA will come back to haunt businesses if they aren't prepared beforehand. For instance, businesses must be able to give access to personal information to verified requests if an employee exercises his/her right to access personal information dating back to Jan 1, 2022.



Does CPRA require training?

Yes, CPRA requires businesses to conduct and provide privacy training to all their personnel that are responsible for handling consumers' or employees' personal information. The CPRA introduces the training requirements in section 1798.130(a)(6), which further cover seven important sections that must be a part of the training, such as section 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and 1798.130.

Colorado Privacy Act



Colorado Privacy Act (CPA)

Colorado Privacy Act (CPA) was signed into law on July 7, 2021 making Colorado the third US state to pass a comprehensive data privacy law. Modeled pretty similarly to the Virginia Data Protection Act (VCDPA), the CPA provides comprehensive privacy rights to state residents of Colorado and imposes a new set of obligations and duties on data controllers managing consumer personal information.

With the increasing importance of privacy in today's digital age, the Colorado Privacy Act represents a major step forward in the protection of personal data for residents of the state. The law is effective from July 1, 2023.

What is the Colorado Privacy Act?

The Colorado Privacy Act, also known as Senate Bill 21-190, is a comprehensive privacy law that was enacted in Colorado on July 7, 2021. This legislation provides significant protections for the personal information of Colorado residents, establishing new standards for the collection, use, and protection of personal data by businesses operating in the state.

Who Needs to Comply with CPA?

Territorial Scope

CPA applies to all data controllers who conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to residents of Colorado - if they match any one or both of the following conditions:

- control or process the personal data of 100,000 consumers or more during a calendar year; or

- derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000 consumers or more.

Exemptions

The following entities are exempt from complying with CPA:

GLBA entities

Financial Institutions or data that is subject to the federal Gramm-Leach-Bliley Act (GLBA) 15 U.S.C. SEC. 6801 ET SEQ., as amended, and implementing regulations, including Regulation P, 12 CFR 1016. are exempt.

COPPA-compliant entities

Controllers and processors that comply with the Children’s Online Privacy Protection Act (COPPA) will be deemed to be in compliance with the CPA.

Air Carriers

An air carrier as defined in and regulated under 49 U.S.C. SEC. 40101 ET SEQ., as amended, and 49 U.S.C. SEC. 41713 are exempt.

National Securities Association

A National Securities Association registered pursuant to the federal “Securities Exchange Act Of 1934”, 15 U.S.C. SEC. 78o-3, as amended, or implementing Regulations are exempt.

Public Utilities and Authorities

Customer data maintained by a public utility as defined in Section 40-1-103 (1)(a)(I) or an authority as defined in Section 43-4-503 (1) is exempt from the law if the data is not collected, maintained, disclosed, sold, communicated, or used except as authorized by state and federal law.

State Institution

Data maintained by a state institution of higher education, as defined in Section 23-18-102 (10), the state, the judicial department of the state, or a county, city, and county, or municipality if the data is collected, maintained, disclosed, communicated, and used as authorized by state and federal law for noncommercial purposes is exempt from the law.

Obligations for Organizations Under CPA

Transparency

A controller must provide consumers with a reasonably accessible, clear, and meaningful privacy notice containing specific information, including categories of data it shares or sells (including for targeted advertising), and means for consumers to exercise their rights and how they can appeal against the denial of their DSRs.

Accountability

A controller must undertake Data Protection Assessments (DPAs) for each processing activity that poses a heightened risk of harm to consumers, protect de-identified data from reidentification and comply with data subject requests made by consumers as well as ensure data processors it

contracts with comply with the duties prescribed under this law.

Purpose Limitation And Data Minimization

Controllers must not collect consumers' unnecessary personal data or process it for purposes beyond what was disclosed to consumers without gaining their consent.

Non-Discrimination

Controllers may not process personal data to discriminate against consumers in violation of state or federal laws that prohibit unlawful discrimination against consumers.

Consent Management




Controllers cannot process sensitive personal data or data of minors unless it has the express consent of the consumer or of the parents/guardians of a minor child, respectively.

Data Security

Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data during both storage and use. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.

Data Subject Rights Under CPA

All consumers may invoke the following rights by sending a verified request to the data controller (in the case of a child, the parent/guardian may send the request on behalf of the child):

-  **Confirm**
The consumer has a right to confirm whether or not a controller is processing his/her personal data.
-  **Access**
The consumer has a right to access the personal data collected and processed about him/her by the data controller.
-  **Rectify**
The consumer has a right to have inaccurate personal data being stored or processed by the data controller be corrected.



Delete

The consumer has the right to have his/her personal data stored or processed by the data controller deleted.



Portability

The consumer has a right to obtain a copy of his/her personal data in a portable, technically feasible, and readily usable format that allows the consumer to transmit the data to another controller without hindrance.



Opt-Out

The consumer has the right to opt out of the processing of 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.

Time period to fulfill DSR request

All data subject rights requests (DSR requests) must be fulfilled by the data controller within a 45-day period.

Extension in the time period

Data controllers may seek an extension of 45 days in fulfilling the request depending on the complexity and number of the consumer's requests.

Denial of DSR request

Data controllers may seek an extension of 45 days in fulfilling the request depending on the complexity and number of the consumer's requests.

Appeal against refusal

Consumers have a right to appeal the decision for refusal of the grant of the DSR request. The appeal must be decided within 45 days, but the period can be extended further by 60 additional days.

Limitation of DSR requests per year

Requests for data portability may be made only twice a year.

Charges

DSR requests must be fulfilled free of charge once a year. Any subsequent request within a 12-month period can be charged.

Authentication

A data controller is not to respond to a consumer request unless it can authenticate the request using reasonably commercial means. A data controller can request additional information from the consumer for the purposes of authenticating the request.

Regulatory Authority

Unlike the VCDPA, which can be enforced only by the Virginia Attorney General, the Colorado Privacy Act can be enforced either by the Attorney General or the District Attorneys.

Any Important Exemptions

The CPA does not apply to:

Data processed in an employment or commercial (business-to-business) context

Personal data processed by a controller, processor, or third party is exempt from the application of this law:

- o If the individual data subject is acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.
- o If the personal data is maintained for employment records purposes.
- o As the emergency contact information of an individual used for emergency contact purposes.

Data processed for free speech or household purposes

Nothing in the law applies to information made available by a third party that the controller has a reasonable basis to believe is protected speech pursuant to applicable law or the processing of personal data by an individual in the course of a purely personal or household activity.

Data processed for internal purposes

Nothing in the law restricts a controller or processor from processing personal data to conduct internal research to improve or repair products, services, or technology or to identify and repair technical errors that impair existing or intended functionality, or to undertake internal operations reasonably aligned with the consumer's expectations for the performance of a service or provision of a product.

Data processed for legal obligations

Nothing in the law restricts a controller or processor from complying with other applicable laws, to claim or defend legal claims or cooperate with government authorities or investigations.

Data processed to protect vital interests or security

Nothing in the law restricts a controller from processing data to protect the vital interests of the consumer or of another individual or 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.

Data processed for public health reasons

Nothing in the law restricts controllers from processing 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 whose personal data are processed; and is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

Penalties for Non-Compliance

Unlike the VCDPA, which can be enforced only by the Virginia Attorney General, t In the event of a notice served by the AG or DAs, the controller will be provided 60 days to fix the violation. A non-compliant business or entity shall be fined up to \$20,000 per violation. he Colorado Privacy Act can be enforced either by the Attorney General or the District Attorneys.

How an Organization Can Operationalize the CPA

Following are some of the important steps that businesses should take to bolster the foundation for compliance with the law:

Streamline and automate the DSR fulfillment framework to speed up consumer verification, personal data linking to its owner, and timely fulfillment processes;

Conduct a regular data protection impact assessment to avoid any significant harm to the consumers via the processing of their personal data;and process or control the personal data of 25,000 consumers or more.

Have pre-built privacy notice templates ready, built on the relevant jurisdictional laws that apply to the business; and

Provide clear opt-out signals on the official website for consumers who wish to exercise their right to opt out of sharing or disclosing their personal information.

Connecticut Data Privacy Act



What is CTDPA?

The Connecticut Senate Bill 6: An Act Concerning Personal Data Privacy and Online Monitoring (CTDPA) is broadly modeled on the Colorado Privacy Act (CPA); however, there are certain differences that set CTDPA apart, such as greater privacy rights for children. Similar to most other privacy legislations, the CTDPA enables consumers to have greater control over the transparency and processing of their personal data, including better visibility into who processes and shares their personal data.

The act was signed into law by Gov. Ned Lamont, D-Conn. on 10th May 2022 and became effective on 1 July 2023. Let's take a quick look at the important provisions of CTDPA along with the underlying rights and obligations.

Who Needs to Comply With the CTDPA

Like most other state privacy laws, the CTDPA also defines its scope, outlining certain types of data and entities which are exempt from the application of its provisions.

Material Scope

The law applies to all personal data that can be identified or linked to an identifiable individual, with the exception of de-identified data or publicly available information.

Medical data

Protected health information regulated under HIPAA, including personal information that can be used to identify patients as well as identifiable personal information for purposes of the federal policy for the protection of human subjects. Personal data that is used or shared in research and information used for public health services is also exempted.

Data covered under the Gramm-Leach-Bliley Act (GLBA)

Personal Information maintained by a covered entity or business associate.

Fair Credit Reporting Act (FCRA) covered data

Personal information collected, maintained, disclosed, sold, or used by a consumer reporting agency only to the extent of such activity being regulated by and authorized under the Fair Credit Reporting Act.

Driver data

Personal information that is subject to compliance with the Driver's Privacy Protection Act.

Family Educational Rights and Privacy Act (FERPA) data: Personal data regulated by the Family Educational Rights and Privacy Act.

Employment data: Personal information pertaining to employment or emergency contact information.

Airline data: Personal data collected, processed, sold, or disclosed as per the Airline Deregulation Act by air carriers.

Territorial Scope

The law applies to businesses that are operating in the state of Connecticut or offering goods and services targeted to Connecticut residents and that during the preceding year:

controlled or processed the personal data of no less than 100,000 consumers, excluding the personal data controlled or processed solely for the purpose of completing a payment transaction or,

controlled or processed the personal data of 25,000 consumers, deriving 25% or more of their gross revenue from selling that data.

Exceptions

The provisions of the law do not apply to:

Government or federal agencies;

Higher educational institutions;

Non-profit organizations, hospitals;

National security associations registered under the Securities Exchange Act;

Covered entities or business associates and financial institutions that are subject to the Gramm-Leach-Bliley Act (GLBA);

Covered entities and business associates as defined by the Health Insurance Portability and Accountability Act (HIPAA).

Obligations for Organizations Under the CTDPA

Like most other state privacy laws, the CTDPA also defines its scope, outlining certain types of data and entities which are exempt from the application of its provisions.

General Principles of Processing

Under the law, the organizations or data controllers must make sure that the personal data or sensitive personal data of a consumer is processed while complying with the following guidelines:

Organizations must practice data minimization and limit the collection of personal data to what is reasonably necessary and adequate for the purpose it was intended;

Personal data shouldn't be processed for purposes that are not reasonably necessary unless the consumer has provided explicit consent;

Organizations must ensure adequate technical and physical security measures are in place for the protection of consumers' personal data;

Organizations must not process the sensitive personal data of consumers without consent;

Organizations are prohibited from treating a consumer unfairly if the consumer exercises any of his or her rights under the bill;

Where an organization has actual knowledge and wilfully disregards that the consumer is at least thirteen years of age but younger than sixteen years of age, it cannot process the personal data of the consumer for purposes of targeted advertising or sell the consumer's personal data without his/her consent;

Similarly, to process the personal data of minors, consent of their parents or guardians is to be obtained as outlined by the Children's Online Privacy Protection Rule;

Organizations should not process personal data violating the state or federal laws prohibiting unlawful discrimination against consumers.

Non-Discrimination

Controllers must not discriminate against a consumer for exercising any of their rights contained in the act by denying them goods or services, charging them different prices, or providing a different level of quality of

goods and services.

However, this requirement does not prohibit a controller from offering a distinct rate (including discounts or product/service at no fee), quality, or selection of a product or service to the consumer, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

Consent Requirements

Under the law, a consumer's consent must be affirmative, freely given, clear, informed, and unambiguous. Also, data controllers must provide an effective mechanism for a consumer to revoke the consent under the law that is as easy as the mechanism through which the consumer provided consent. Upon revocation of the consent, the controller should cease to process the data as soon as practicable but no later than fifteen (15) days after the receipt of such request.

Moreover, the law prohibits organizations from using any dark patterns for consent. It defines dark patterns as user interfaces designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

Consent will not be deemed valid if it is acceptance of general or broad terms of use. Lastly, hovering, muting, pausing, or closing a given piece of content will also not be considered consent.

Privacy Notice Requirements

The controllers are required to present a clear and accessible privacy notice on their website or application, including the following information:

- the categories of personal data collected on them;
- the purpose for processing their personal data;
- the categories of personal data shared with any third party;
- the process through which the consumers can exercise their rights, including the appeal process regarding the refusal of a consumer request;
- An active electronic mail address through which the consumer can contact the controller.

Processor/Service Provider Agreements

The law mandates that there should be an agreement between a controller and a processor governing the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract should be binding and clearly set forth instructions for processing data, the nature, and purpose of processing, the type of data subject to processing, the duration of the processing, and the rights and obligations of both parties.

Also, the contract must also require that the processor:

- to ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

- at the controller's direction, to delete or return all personal data to the controller as requested at the end of the provision of services unless retention of the personal data is required by law;

- upon the reasonable request of the controller, to make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in the act;

- after providing the controller an opportunity to object, to engage any subcontractor in line with a written contract to meet the obligations of the processor with respect to the personal data; and

- to allow and cooperate with reasonable assessments by the controller or the controller's designated assessor using an appropriate and accepted control standard or framework and assessment procedure for such assessments and subsequently provide a report of such assessment to the controller upon request.

Data Protection Assessment

The law requires the controllers to conduct data protection impact assessment (DPA) for processing activities that present a heightened risk of harm to consumers, including the following:

- the processing of personal data for targeted advertising;

- the sale of personal data;

- the processing of personal data for the purposes of profiling presents a reasonably foreseeable risk, such as unfair or deceptive treatment, intrusion in the private affairs of the consumer which would be considered offensive to a reasonable person, or a financial, physical,

or reputational injury to a consumer;

the processing of sensitive data.

The DPA may take into account any reasonable expectation of the consumer, use of any de-identified data, or the context of processing and relationship between the controller and the consumer whose personal data is to be processed.

The law further requires data controllers to maintain a record of DPAs for auditing purposes by the Attorney General. However, such records must remain confidential and exempt from any disclosure under the Freedom of Information Act. In the case where any information contained in a data protection assessment that is disclosed to the Attorney General includes information subject to the attorney-client privilege or work product protection, such disclosure would not constitute a waiver of such privilege or protection.

The requirement to conduct DPA is only applicable for processing activities created or generated after July 1, 2023.

Data Subject Rights Under CTDPA

Data subject rights are one of the most important components of every privacy law. The CTDPA provides the following rights to the consumers:



Right to Confirm Processing and Access

The consumers have a right to confirm whether or not a controller is processing their personal data and accessing such personal data unless such confirmation or access would require the controller to reveal a trade secret.



Right to Correct

The consumers have a right to request the controller to fix any inaccuracies in the personal data they have collected on the consumer. However, this right is subject to the nature of the personal data collected and its processing purpose.



Right to Delete

The consumers have a right to delete their personal data, which is provided to or obtained about them by the controller.



Right to Obtain a Copy of Personal Data

The consumers have a right to obtain a copy of their personal data from the controller in a portable and readily usable format and in a manner that makes it feasible for the consumer to forward the data to any other controller or business without any hindrances.



Right to Opt-Out

Consumers have a right to opt-out from the processing of their personal data for any or all of the following purposes:

- Targeted advertising,
- Sale of personal data,
- Automated profiling.

A consumer can also designate an authorized agent to exercise their right to opt-out from processing personal data on their behalf.

The controllers must be able to recognize and honor a global opt-out preference signal received from a platform, technology, or mechanism with the consumer's consent. It is to be noted, however, that these platforms should:

- Not unfairly disadvantage another controller and be consumer-friendly and easy to use by an average consumer; or
- Not use any default setting but rather require an affirmative, freely given, and unambiguous choice to opt-out of any processing of such consumer's personal data;
- Be consistent with any other similar platform required by any federal or state law;
- Allow the consumer to determine the residency of the consumer easily and whether the consumer has made a legitimate request to opt-out of the sale of their personal data or targeted advertising.

Time Period to Fulfill DSR Request

A controller must respond to all DSR requests within forty-five (45) days after receiving them. A further extension of forty-five (45) days is possible when reasonably necessary, considering the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five (45) days period.

Charges for DSR Request Fulfillment

Information provided in response to a consumer request must be provided by a controller, free of charge, once per consumer during any 12-month period. If the consumer requests are manifestly unfounded, excessive, or repetitive, then the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request.

Denial of DSR Request

If a controller is unable to authenticate a request to exercise any of the rights listed in this act by using commercially reasonable efforts, the controller is not obligated to comply with a request and should provide notice to the consumer of such a situation. Similarly, a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that such a request is fraudulent. In this case, the controller should send a notice to the consumer disclosing that the controller believes such a request is fraudulent, why the controller believes such a request is fraudulent, and that the controller shall not comply with such request.

Appeal Against Refusal

The process established for the consumer to appeal the controller's refusal to take action must be available in a conspicuous manner, without causing additional cost to the consumer, while also being similar to the process of making other consumer requests. The controller must inform the consumer of any action taken or not taken concerning their appeal within sixty (60) days of receiving the appeal, alongside a written explanation of the reasons behind the decision. If the appeal is denied, the controller shall ensure they communicate an online mechanism to the consumer allowing them to contact the Attorney General's office to submit an official complaint.

Regulatory Authority

The Connecticut Attorney General (AG) is the exclusive regulatory authority responsible for the enforcement of the law.

Between July 1, 2023, and December 31, 2024: the Attorney General must send a notice of violation to the controller if the AG believes that a cure is possible before taking any action pursuant to the provisions of the law. If the controller fails to cure the violation within a 60-day period, the AG may proceed with the enforcement actions.

Moreover, after February 1, 2024: The AG shall submit a report to the General Assembly detailing the number of

notices of violation the AG has sent, the nature of the violation, and the number of cured violations during the 60-day cure period.

Further, from January 1, 2025, the AG may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation, consider the following:

- the number of violations;
- the size and complexity of the controller or processor;
- the nature and extent of the controller's or processor's processing activities;
- the substantial likelihood of injury to the public;
- the safety of persons or property; and
- whether such alleged violation was likely caused by human or technical error.

Any Important Exemptions

The Act includes some substantive exemptions, where no provisions in the act can be used to restrict a controller's or processor's ability to:

- Comply with federal, state, or municipal ordinances or regulations;
- Cooperate with law enforcement agencies concerning conduct or activity;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a product or service specifically requested by a consumer;
- Perform contractual obligations with a consumer, including fulfilling the terms of a written warranty;
- Protect an interest that is essential for the life or physical safety of the consumer or another individual;
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, and malicious activities;
- Engage in public or peer-reviewed scientific or statistical research in the public interest that provides substantial benefits that do not exclusively accrue to the controller or has expected benefits that outweigh privacy risks, and whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

Assist another controller, processor, or third party with the fulfillment of any of the obligations under this act;

Process personal data for reasons of public interest in the area of public health, community health, or population health;

Collect, use, or retain data for internal use to improve or repair products, services, or technology, effectuate a product recall, or identify and repair technical errors that impair existing or intended functionality.

Moreover, the obligations imposed on controllers or processors under the law shall not apply where compliance by the controller or processor would violate an evidentiary privilege under the laws of the State of Connecticut.

Penalties For Non-Compliance

Any violation of the law is an unfair trade practice under the Connecticut Unfair Trade Practices Act (CUTPA), and the violator may face civil penalties of up to \$5,000 per willful violation as well as other equitable remedies pursuant to the CUTPA, including restitution, disgorgement, and injunctive relief.

How an Organization Can Operationalize the CTDPA

Following are some of the important steps that businesses should take to bolster the foundation for compliance with the law:

Streamline and automate the DSR fulfillment framework to speed up consumer verification, personal data linking to its owner, and timely fulfillment processes;

Conduct a regular data protection impact assessment to avoid any significant harm to the consumers via the processing of their personal data;

Have pre-built privacy notice templates ready, built on the relevant jurisdictional laws that apply to the business; and

Provide clear opt-out signals on the official website for consumers who wish to exercise their right to opt out of sharing or disclosing their personal information.

Delaware Personal Data Privacy Act



What is DPDPA?

The Delaware Personal Data Privacy Act (DPDPA) – HB 154 was approved by the Delaware General Assembly on June 30, 2023. If signed into law by Governor John Carney, Delaware would become the twelfth US state to have comprehensive data privacy legislation and the seventh state to pass one in 2023 only, joining Iowa, Indiana, Montana, Tennessee, Texas, and Oregon.

With some notable differences, the DPDPA closely resembles the Connecticut Data Privacy Act (CTDPA). The law shall become effective on January 1, 2025, if signed by the governor before or on January 1, 2024. Otherwise, the law shall go into effect on January 1, 2026.

Who Needs to Comply with DPDPA

Material Scope

DPDPA applies to those who do business in Delaware or who produce goods or services that are targeted to Delaware citizens and who, during the preceding calendar year, did any of the following:

Controlled or processed the personal data of at least 35,000 customers, except those whose data was controlled or processed only to facilitate a payment transaction; and

Controlled or processed the personal data of at least 10,000 customers and derived more than 20% of their gross revenue from the sale of personal data.

Exemptions

The law exempts certain types of entities and data from its application. The following entities do not fall under the scope of the law:

Any government body or a political subdivision of Delaware, excluding any institution of higher education;

Any financial institution or affiliate of a financial institution that is subject to the Gramm Leach Bliley Act (GLBA);

Any nonprofit organization (NPO) dedicated exclusively to preventing and addressing insurance crime; and

A futures association registered under the Commodity Exchange Act or a national securities association registered under the Securities Exchange Act.

DPDPA does not apply to the following information and data:

Data covered under medical laws

Many forms of health information, records, data, and documents are protected and covered under HIPAA or other federal or state medical/healthcare laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting to the extent the activity is authorized and regulated by the federal Fair Credit Report Act (FCRA);

GLBA data

Financial data subject to Title V of the federal Gramm-Leach-Bliley Act;

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

Employment data

Personal data maintained for employment records;

ADA data

Personal data collected, processed, sold, or disclosed in relation to price, route, or service under the Airline Deregulation Act (ADA), to the extent the provisions of DPDPA are preempted by ADA.

Abuse data maintained by NPOs

Personal data of a victim of or witness to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking that is collected, processed, or maintained by an NPO that provides services to such a victim or witness.

Obligations for Organizations Under DPDPA

Data Minimization and Purpose Limitation

Controllers must maintain transparency in their data collection practices and only collect personal data that is adequate, relevant, and reasonably necessary for the processing purposes notified to the consumer.

Except as otherwise permitted by DPDPA, the controller must not, without the consumer's consent, process personal data for any purposes which are neither reasonably necessary nor consistent with the initially declared purposes.

Consent Requirements

To comply with DPDPA requirements regarding acquiring parental consent with respect to a child consumer, controllers, and processors must comply with the verified parental consent standards of COPPA.

Controllers and processors must not process consumers' sensitive data without obtaining their consent or, when processing sensitive data concerning a known child, without obtaining the child's parent or legal guardian's consent.

Additionally, consumers must be provided with a method by which they can withdraw their consent in a similar manner as the method they originally used, and upon such withdrawal, the controllers stop processing the data as soon as is reasonably possible but no later than 15 days after receiving the request.

Privacy Notice Requirements

Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following:

The categories of personal data that the controller processes;

The reason why personal data is processed;

How consumers can exercise their rights as consumers, including how to appeal a controller's decision about a consumer's request;

The types of personal information that the controller exchanges with third parties, if any;

The types of third parties with whom the controller shares personal data, if any;

The consumer may use a working email address or other online contact method to contact the controller.

A controller must establish and describe in the privacy notice one or more secure and reliable means for consumers to submit a request to exercise their consumer rights. These methods must consider how consumers often communicate with the controller, the requirement for secure and dependable transmission of such requests, and the controller's capacity to confirm the consumer's identification.

Controllers must provide a prominent link on the organization's website that directs users to a page on another website where they can choose not to receive targeted advertisements or have their personal information sold.

Opt-out Requirements

Controllers must enable consumers to opt-out of any processing of their personal data for the purpose of targeted advertising or any sale of their personal data by sending an opt-out preference signal to the controller with their consent via a platform, technology, or mechanism indicating their desire to refuse any such processing or sale. However, this requirement shall come into force no later than one year after the DPDPA's effective date. Such a platform, technology, or mechanism must:

Not disadvantage another controller unfairly;

Refrain from using default settings and instead demand that users explicitly, freely, and unambiguously opt-out of having their personal data processed;

Be user-friendly and simple to use by average consumers;

Be as compliant with any other comparable platform, technology, or mechanism mandated by any federal or state law or regulation as is practicable;

Enable the controller to determine, in a reasonable amount of time, whether the consumer is a Delaware resident and has made a valid request to opt-out of any sales of their personal data or targeted advertising.

Security Requirements

Controllers must 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.

Non-Discrimination Requirements

Controllers must not process personal data violating Delaware laws and federal laws prohibiting unlawful discrimination. Additionally, controllers must not discriminate against a consumer for exercising any of their rights, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

Targeted Advertising Requirements

In situations where a controller has actual knowledge or willfully disregards the fact that the consumer is at least thirteen years of age but younger than eighteen years of age, the controller must not process the personal data of a consumer for the purposes of targeted advertising or sell the consumer's personal data without the consumer's consent.

If a controller sells personal data to third parties or utilizes personal data for targeted advertising, it must disclose this processing to consumers clearly and noticeably, together with how they can exercise their right to object to the processing.

Data Protection Assessment

Data protection assessments must be conducted and documented regularly for each of the controller's processing activities that present a heightened risk of harm to a consumer. This requirement applies to controllers that control or process the data of at least 100,000 consumers, excluding data controlled or processed solely to complete a payment transaction. Processing activities that put consumers at heightened risk of harm include:

The processing of personal data for the purposes of targeted advertising.

The sale of personal data.

The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following:

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.

Other substantial injuries to consumers.

The processing of sensitive data.

Data protection assessments must determine and compare the potential risks to the consumer's rights associated with the processing, as mitigated by safeguards that the controller can use to mitigate those risks, to the benefits that may result, directly or indirectly, to the controller, the consumer, other stakeholders, and the public. Any such data protection assessment by the controller must consider the context of the processing, the relationship between the controller and the consumer whose personal data will be processed, the use of de-identified data, and consumers' reasonable expectations.

The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller must make the data protection assessment available to the Attorney General. A controller must also conduct a data protection assessment that is reasonably equivalent in scope and impact to a previous data protection assessment. Data protection assessment requirements are not retroactive and must be performed for processing activities established or generated on or after the six-month mark after the DPDPA's effective date. A data protection evaluation is private and cannot be disclosed.

Disclosure of Pseudonymous or De-identified Data

While disclosing pseudonymous data or de-identified data, controllers must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and must take appropriate steps to address any breaches of those contractual commitments. The determination of the reasonableness of such oversight and the appropriateness of contractual enforcement must take into account whether the disclosed data includes data that would be sensitive data if it were re-identified.

Data Processor Responsibilities

Assistance to Controller

A processor must follow a controller's instructions to assist the controller in carrying out its obligations. The processor's role in supporting the controller is to:

Enable the controller to respond to consumer requests using techniques that, to the degree practically possible, make use of appropriate technological and organizational measures, taking into account how the processor processes personal data and the information at its disposal;

Implement reasonable administrative, technical, and physical security measures, considering how the processor utilizes the data and information at its disposal to protect the security and privacy of the personal data it processes;

Provide the controller with the necessary data to conduct and document data protection assessments.

Processing Under Contract

The processor and the controller must enter into a contract before the processor can process personal data on the controller's behalf. The contract must:

Be legitimate and enforceable against both parties;

Clearly specify the types of data that will be processed, how the processing will be carried out, its nature, and duration;

Clearly explain each party's responsibilities and rights;

Ensure that each stakeholder handling personal data is committed to ensuring its confidentiality;

Require that the processor deletes the personal data or return it to the controller upon request from the controller or completion of the services unless the processor is required by law to keep the data;

Require the processor to disclose all information necessary for the controller to confirm that the processor has complied with all of its duties available to the controller upon request from the controller;

Require the processor to enter into a subcontract with a person they engage to assist with processing personal data on their behalf, and the subcontract must include a clause requiring the subcontractor to uphold the processor's duties under the processor's contract with the controller; and

Enable the assessment of the processor's policies and organizational

and technical measures for complying with its obligations by the controller, the controller's designee, or a qualified and independent person the processor engages in accordance with an appropriate and accepted control standard, framework or procedure. Require the processor to cooperate with the assessment and report the assessment results to the controller upon the controller's request.

Data Subject Rights



Right to Confirm

Consumers have the right to confirm whether a controller is processing the consumer's personal data and the right to access such personal data unless such confirmation or access would require the controller to reveal a trade secret.



Right to Correct

Consumers have the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing the consumer's personal data.



Right to Delete

Consumers have the right to delete personal data provided by or obtained about the consumer.



Right to Obtain a Copy

Consumers have the right to obtain a copy of their personal data processed by the controller in a portable and, to the extent technically possible, easily usable format that enables them to transmit the data to another controller without difficulty if the processing is automated.



Right to Know

Consumers have the right to obtain a list of the categories of third parties to which the controller has disclosed their personal data.



Right to Opt-Out

Consumers have the right to opt-out of the processing of personal data for any of the following purposes:

Targeted advertising.

The sale of personal data.

Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

How can consumers exercise their rights

Consumers can exercise their rights through a safe and reliable method that the controller has created and made clear to the consumer in the controller's privacy notice. A consumer can designate an authorized agent to exercise their right to object to processing their personal data. If a known child's personal data is being processed, the parent or legal guardian may exercise the consumer's rights on the child's behalf. The consumer's guardian or conservator may exercise these rights on the consumer's behalf when processing personal data on a consumer who is under guardianship, conservatorship, or other protective arrangement.

A consumer may designate an authorized agent to act on the consumer's behalf to opt-out of processing such consumer's personal data. The consumer may designate such authorized agent by way of, among other things, a platform, technology, or mechanism, including an Internet link or a browser setting, browser extension, or global device setting, indicating such consumer's intent to opt out of such processing. Platforms, technologies, or other mechanisms may serve as agents to communicate the consumer's decision to opt-out.

Controller's response to data subject rights

The controller must respond to a consumer's request without undue delay but not later than 45 days after receiving the request. When it is deemed reasonable given the complexity and volume of the consumer's requests, the controller may extend the response period by an additional 45 days, as long as they notify the consumer of any such extension within the initial 45-day response period and explain the justification for it.

When a controller does not respond to a consumer's request, the controller is required to give the consumer notice of the reason(s) for the refusal to act as well as information on how to appeal the decision without undue delay, but no later than 45 days after receiving the request.

A controller must provide information in response to a consumer request free of charge once per consumer during any 12-month period. However, if a request from the consumer is clearly unjustified, excessive, or recurrent, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request, or the controller may choose not to act on the request. However, the controller bears the burden of proving the request's manifestly unfounded, excessive, or repetitive nature.

A controller is not required to comply with a consumer request submitted if the controller cannot authenticate the request using commercially reasonable efforts. Instead, the controller may request that the consumer

provide any additional information reasonably required to authenticate the consumer and the consumer's request.

A controller is not required to authenticate an opt-out request; however, a controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that such a request is fraudulent. In such a case, the controller must notify the person who made such a request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent, and that such controller shall not comply with such request.

Lastly, a controller must comply with an opt-out request made by an authorized agent if the controller can confirm the consumer's identity and the authorized agency's legitimacy to act on the consumer's behalf using commercially reasonable efforts.

Appeal process

A controller must establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section.

A controller must give the consumer written notice of all actions taken or not done in response to an appeal within 60 days of receiving the appeal. This notice must include a written explanation of the decisions. If the appeal is turned down, the controller must provide the consumer access to an online complaint form, if one is available, or another way to contact the Department of Justice.

Regulatory Authority

The Department of Justice (DOJ) has enforcement authority over DPDPA and may investigate and prosecute violations.

Limitations

The obligations imposed under DPDPA do not restrict a controller's or a 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;

Investigate, establish, exercise, prepare for, or defend legal claims;

Provide a product/service specifically requested by a consumer, perform a contract, fulfill the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another natural person;

Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity;

Engage in public or peer-reviewed scientific research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines:

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

whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; and

Assist another controller, processor, or third party with their obligations under DPDPA. 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;

Investigate, establish, exercise, prepare for, or defend legal claims;

Provide a product/service specifically requested by a consumer, perform a contract, fulfill the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or

another natural person;

Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity;

Engage in public or peer-reviewed scientific research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines:

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

Assist another controller, processor, or third party with their obligations under DPDPA.

Nothing under DPDPA may restrict a controller or processor's ability to collect, use, or retain data for internal use only to do any of the following:

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 internal operations that are reasonably aligned with the consumer's expectations or 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.

Similarly, any obligations placed on a controller or a processor under DPDPA do not apply if compliance by the controller or processor would violate an evidentiary privilege under Delaware laws or adversely affect the rights or freedoms of a person.

Penalties for Non-Compliance

Any violation of the provisions of the law is an unlawful practice within the meanings of section 2513 of Chapter 25 of Title 6 of the Delaware Code. However, before initiating any action for a violation of DPDPA's provisions, the DOJ shall issue a notice of violation to the controller during the period starting on the effective date of

DPDPA and ending on December 31, 2025, if the DOJ determines that a cure is possible. The DOJ may bring an enforcement action if the controller doesn't correct the violation within 60 days of receiving the notice of violation.

Beginning on January 1, 2026, the DOJ may take into account all of the following when deciding whether to give a controller or processor an opportunity to correct an alleged violation of any clause:

- The number of violations.
- The size and complexity of the controller or processor.
- The nature and extent of the controller's or processor's processing activities.
- The substantial likelihood of injury to the public.
- The safety of persons or property.
- Whether such alleged violation was likely caused by human or technical error.
- The extent to which the controller or processor has violated this or similar laws in the past.

How an Organization Can Operationalize DPDPA

Organizations can operationalize the HB 154 – Delaware Personal Data Privacy Act (DPDPA) by:

- Establishing clearly defined policies and procedures for processing data in compliance with DPDPA's provisions;
- Developing clear and accessible understandable privacy notices that comply with DPDPA's requirements;
- Obtaining explicit consent from consumers before processing their sensitive personal data;
- Developing a robust framework for receiving and processing data requests, complaints, and appeals from consumers; and
- Train employees who handle the consumers' data on the organization's policies and procedures, as well as the requirements of the DPDPA.

Florida Digital Bill of Rights



What is the Florida Digital Bill of Rights?

On June 6, 2023, Florida's Governor Ron DeSantis signed Senate Bill 262 into law, which contains the Florida Digital Bill of Rights (FDBR), making Florida the latest US state to have a comprehensive data privacy law. The law is set to take effect from July 1, 2024.

A billion-dollar gross revenue threshold makes the FDBR reach far more conservative than the other US state data privacy laws and makes it inapplicable to most of the small to medium-sized businesses operating in the state of Florida.

Who Needs to Comply with the FDBR

Material Scope

The law applies only to a person who:

- conducts business in Florida or produces a product or service used by the residents of Florida; and
- processes or engages in the sale of personal data.

A business, including a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity, is a 'controller' and subject to most of the obligations under the FDBR if it:

- Is organized or operated for the profit or financial benefit of its shareholders or owners;
- Conducts business in this state;
- Collects personal data about consumers, or is the entity on behalf of which such information is collected;
- Determines the purposes and means of processing personal data about consumers alone or jointly with others;
- Makes more than \$1 billion in global gross annual revenues; and
- Meets at least one of the following:
 - Derives 50 percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online;

Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation. This excludes a motor vehicle or speaker or device associated with or connected to a vehicle that is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or

Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

Exemptions

The law does not apply to:

a state agency or a political subdivision of Florida;

a financial institution subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);

a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services (HHS), established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH);

a nonprofit organization;

a postsecondary educational institution; and

the processing of personal data:

- o By a person in the course of a purely personal or household activity; and
- o Solely for measuring or reporting advertising performance, reach, or frequency.

The following information is also exempt from the application of the FDBR:

Medical data covered under any medical laws

Many forms of health information, records, data, and documents protected and covered under HIPAA or other federal or state medical/healthcare laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting to the extent the activity is authorized and regulated by the federal Fair Credit Report Act (FCRA);

GLBA data

Financial data subject to Title V of the federal Gramm-Leach-Bliley Act;

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

Employment data

Personal data maintained for employment records;

ADA data

Personal data collected, processed, sold, or disclosed in relation to price, route, or service as those terms are used in the Airline Deregulation Act (ADA), 49 U.S.C. ss. 40101 et seq., by entities subject to that act, to the extent the provisions of FDBR are preempted by 49 U.S.C. s. 41713;

Personal data used for payment

Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provided solely to facilitate short-term, transactional payment processing for the purchase of products or services; and

Personal data shared between a manufacturer and distributors

Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as

long as such personal data is used solely for advertising, marketing, or servicing the product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors.

Obligations for Organizations Under FDBR

Data Minimization and Purpose Limitation

A controller must limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer.

Security Measures

To protect the confidentiality, integrity, and accessibility of personal data, the controllers must establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.

Non-Discrimination Requirements

Controllers must not process the consumers' personal data violating the state or federal laws prohibiting unlawful discrimination against consumers.

Further, the controllers must not discriminate against a consumer for exercising any of their rights, including being denied products or services, being charged a different price or rate for the same goods or services, or being provided with inferior goods or services. If the consumer gives the controller prior consent that specifically outlines the key conditions of the financial incentive program, and as long as the incentive practices are not unfair, unreasonable, coercive, or usurious in nature, the controller may offer financial incentives, including payments to consumers as compensation, for the processing of personal data.

Consent Requirements

Without the consumer's consent, controllers are not allowed to process a consumer's personal data for a reason that is neither reasonably necessary nor compatible with the purpose for which the data was originally collected.

Additionally, a controller cannot process sensitive data about a consumer without the consumer's consent. The federal Children's Online Privacy Protection Act (COPPA) must be followed when processing sensitive data of a known child.

Methods for Submission of DSR Requests

Controllers must establish two or more methods to enable the consumers to submit a request to exercise their consumer rights under the FDBR. Such methods must be secure, reliable, and clearly and conspicuously accessible and must take into account the following:

- the ways in which the consumers normally interact with the controller;
- the necessity for secure and reliable communications of those requests; and
- the ability of the controller to authenticate the identity of the consumer making the request.

Privacy Notice Requirements

Controllers must provide consumers with a reasonably accessible and clear privacy notice, updated at least annually, that includes all of the following information:

- The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;
- The purpose of processing personal data;
- How consumers may exercise their rights, including the process by which they may appeal a controller's decision concerning the consumer's request;
- If applicable, the categories of personal data that the controller shares with third parties;
- If applicable, the categories of third parties with whom the controller shares personal data; and
- A description of the methods by which consumers can submit requests to exercise their rights.

When engaging in the sale of sensitive personal data

If a controller engages in the sale of personal data that is sensitive data, the controller must provide the following notice:

NOTICE: This website may sell your sensitive personal data.

When engaging in the sale of personal data that is biometric data

If a controller engages in the sale of personal data that is biometric data, the controller must provide the following notice:

NOTICE: This website may sell your biometric personal data.

When processing personal data for targeted advertising or selling it to third parties, a controller must make that processing transparent to consumers and make it easy for them to exercise their right to opt-out. Without informing the consumer, a controller cannot obtain more categories of personal information or use the information for new uses.

Requirements for Controllers Operating Search Engines

Controllers operating a search engine must make available, in an easily accessible location on the web page, which does not require a consumer to log in or register to read, an up-to-date plain language description of the main parameters that are individually or collectively the most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed, nor is any other information that, with reasonable certainty, would enable deception of or harm to consumers by manipulating search results.

Data Protection Impact Assessment

Controllers must carry out and record a data protection assessment (DPA) for each of the following personal data processing activities generated on or after July 1, 2023:

Processing personal data for the purposes of targeted advertising;

Sale of personal data;

Processing of personal data to profile consumers, especially if the profiling presents a reasonably foreseeable risk of:

- o Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- o Financial, physical, or reputational injury to consumers;
- o Physical or other intrusions upon the solitude or seclusion, or the private affairs or concerns, of consumers; or

- o Other substantial injuries to consumers;

Processing sensitive data; and

Any other processing of personal data that presents a heightened risk of harm to consumers.

A DPA must do all of the following:

Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce such risks;

Factor into the assessment the following:

- o The use of deidentified data;
- o The reasonable expectations of consumers;
- o The context of the processing; and
- o The relationship between the controller and the consumer whose personal data will be processed.

A DPA carried out by the controller to comply with other regulations may also be used for the purposes of FDBR if the DPA has a reasonably comparable scope and effect to a DPA conducted under the provisions of FDBR and the controller may address a comparable set of processing operations which include similar activities within a single DPA.

Deidentified or Pseudonymous Data Requirements

A controller in possession of de-identified data must do all of the following:

take reasonable steps to ensure that the data cannot be used to identify a specific individual;

maintain and use the data in de-identified form and must not attempt to re-identify the data, except that the controller may attempt to re-identify the data solely for the purpose of determining whether its de-identification processes satisfy the requirements of the FDBR;

contractually obligate any recipient of the de-identified data to comply with the provisions of the FDBR; and

implement business processes to prevent the inadvertent release of deidentified data.

Data Processor Responsibilities

Assistance to Controller

A processor is required to comply with a controller's instructions and assist the controller in fulfilling its responsibilities, which include:

assisting the controller in responding to consumer rights requests;

assisting the controller in complying with the requirement pertaining to the security of processing personal data and the notification of a system security breach by taking into account the nature of processing and the information at the processor's disposal; and

providing the controller with the data necessary to conduct and document data protection assessments.

Processing Under Contract

The processor must be required to process the personal data on behalf of the controller in accordance with the terms of the contract between the controller and the processor. The contract must include all of the following information:

clear instructions for processing data;

the nature and purpose of the processing;

the type of data subject to processing;

the duration of the processing;

the rights and obligations of both the parties; and

a requirement that the processor shall:

- o ensure the confidentiality of the personal data;
- o delete or return the personal data to the collector on the direction of the controller unless retention of personal data is required by the law;

- o upon reasonable request from the controller, make available all the information in possession necessary to demonstrate compliance with its obligations;
- o allow the controller to conduct an assessment, or arrange for a qualified and independent assessor to conduct an assessment, of the processor's policies and technical and organizational measures in support of the processor's obligations; and
- o engage any subcontractor or agent through a written instrument requiring them to fulfill obligations towards the personal data.

Data Subject Rights Under FDBR



Right to Access

Consumers have the right to access their personal data.



Right to Confirm

Consumers have the right to confirm whether a controller is processing their personal data.



Right to Correct Inaccuracies

Consumers have the right to correct inaccuracies in their personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data.



Right to Delete

Consumers have the right to delete any or all personal data provided by or obtained about them.



Right to Obtain a Copy

Consumers have the right to obtain a copy of their personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format.



Right to Opt-Out of the Processing

Consumers have 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 a decision that produces a legal or similarly significant effect concerning the consumer.



Right to Opt-Out of the Collection of Sensitive Data

Consumers have the right to opt-out of the collection of sensitive data, including precise geolocation data or the processing of sensitive data.



Right to Opt-Out of the Collection of Personal Data

Consumers have the right to opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

How to exercise consumer rights

Consumers have the right to exercise their rights at any time by making a request in writing to the controller that specifically lists the rights they want to exercise. A parent or legal guardian of the child may exercise these rights on the child's behalf concerning the processing of the personal data of a known child.

Controller's response to data subject rights

The controller must fulfill any request made by a consumer to exercise their rights. A controller must reply to a consumer request promptly but no later than 45 days after the date the request was received. As long as the controller notifies the consumer of the extension within the initial 45-day response period, along with the justification for the extension, the controller may extend the response period once by an additional 15 days when it is deemed reasonably necessary, taking into account the complexity and volume of the consumer's requests.

If a controller declines to act on a consumer's request, the controller must promptly notify the consumer of the reason(s) why and give instructions on how to appeal the decision. This notification must occur no later than 45 days after the date the request was received.

To verify the consumer and the consumer's request, a controller must reasonably attempt to request that the consumer give any additional information that is required. A controller can decline a consumer's request and require that the consumer update his or her own personal data through a self-service mechanism if the controller keeps such a system in place to allow a consumer to correct particular personal data. The notice that the controller has complied with the consumer's request must be given to the consumer within 60 days of receiving the request.

A controller must respond to a consumer request for information or action

without charge at least twice per year for each consumer. Consumers may be charged a fair fee to offset the administrative costs of complying with clearly unjustified, excessive, or recurrent requests, or the controller may choose not to act on the request altogether. The obligation of proving that a request is plainly baseless, disproportionate, or recurrent rests with the controller.

Appeal process

When a consumer receives a decision from a controller, the controller must provide a procedure for the consumer to appeal to the controller's refusal to act on the request within a reasonable amount of time. The procedure for filing an appeal must be readily accessible, similar to the procedure for taking steps to exercise consumer rights. Within 60 days of the appeal's receipt, the controller must provide written notice to the consumer of any action taken or not taken in response to the appeal, along with a documented justification for the decision.

Regulatory Authority

The Florida Department of Legal Affairs (DLA) is the regulatory authority responsible for enforcing the law.

If the DLA has reason to believe that a person is in violation of the FDBR, the department may notify the person of the violation and may bring an action against such person for an unfair or deceptive act or practice. After the DLA has notified a person in writing of an alleged violation, the DLA may grant a 45-day period to cure the alleged violation; however, no cure period is granted for the violations involving Florida consumers who are known children. If the alleged violation is cured to the satisfaction of the DLA and proof of such cure is provided to the DLA, the DLA may not bring an action for the alleged violation but, at its discretion, may issue a letter of guidance that indicates that the person will not be offered a 45-day cure period for any future violations. However, if the person fails to cure the alleged violation within 45 calendar days, the department may bring an action on behalf of a consumer against such person for the alleged violation.

Limitations

The obligations imposed under FDBR do not restrict a controller's or a 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;

Investigate, establish, exercise, prepare for, or defend legal claims;

Provide a product/service specifically requested by a consumer, perform a contract, fulfill the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis;

Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity;

Preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security;

Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines if:

- o Deletion of the information is likely to provide substantial benefits to the controller;
- o The expected benefits of the research outweigh the privacy risks;
- o The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification;

Assist another controller, processor, or third party with their obligations under the FDBR;

Provide personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of Florida as part of a privileged communication;

Disclose personal data disclosed when a consumer uses or directs the controller to disclose information to a third party intentionally or uses the controller to interact with a third party intentionally. An intentional interaction occurs when the consumer intends to interact with the third party through one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party; and

Transfer personal data to a third party as an asset that is part of a merger, an acquisition, a bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared in a manner consistent with this part. If a third party materially alters

The requirements imposed on controllers and processors under this part may not restrict a controller's or processor's ability to collect, use, or retain data to do any of the following:

Conduct internal research to develop, improve, or repair products, services, or technology.

Effect a product recall.

Identify and repair technical errors that impair existing or intended functionality.

Perform internal operations that are:

- o Reasonably aligned with the expectations of the consumer;
- o Reasonably anticipated based on the consumer's existing relationship with the controller;
- o 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.

Similarly, any obligations placed on a controller or a processor under FDBR do not apply if:

compliance by the controller or processor would adversely affect the rights or freedoms of a person, including the right to free speech; and

compliance by the controller, processor, or third party requires them to disclose a trade secret.

Penalties for Non-Compliance

A violation of the FDBR is an unfair and deceptive trade practice actionable solely by the DLA. The DLA may collect a civil penalty of up to \$50,000 for each violation of the provisions of the FDBR. Civil penalties may be tripled for any of the following violations:

A violation involving a Florida consumer who is a known child. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age.

Failure to delete or correct the consumer's personal data after receiving an authenticated consumer request or directions from a controller to delete or correct such personal data, unless an exception to the requirements to delete or correct such personal data applies.

Continuing to sell or share the consumer's personal data after the consumer chooses to opt-out.

How an Organization Can Operationalize the FDBR

Organizations can operationalize the FDBR by:

- Establishing policies and procedures for processing data in compliance with the requirements of the FDBR;
- Developing clear and accessible privacy notices in compliance with the requirements of the FDBR;
- Obtaining informed consent from individuals before processing their sensitive personal data;
- Developing a robust framework for receiving and processing data requests and complaints from consumers; and
- Training employees who handle the consumers' data on the organization's policies and procedures, as well as the requirements of the FDBR.

Indiana's Consumer Data Protection Act



What is ICDPA?

Indiana became the seventh state in the United States of America to have its own data protection regulation. Modeled closely on the Virginia Consumer Data Protection Act (VCDPA), Indiana's Senate Bill 5 (SB 5), better known as the Indiana Consumer Data Protection Act (ICDPA), passed the Senate vote 49-0 in February 2023.

Then on April 11, 2023, the House passed an amended version of the regulation, with the Senate concurring with the amendments. Finally, Governor Eric Holcomb signed the bill into law on May 01, 2023. The ICDPA contains all the necessary provisions to protect consumers' data privacy rights while laying down strict obligations for all subject organizations.

The law will come into effect from January 1, 2026.

Who Needs to Comply with the ICDPA

Material Scope

The ICDPA applies to persons conducting business in Indiana or producing products and services targeted to Indiana residents who meet the following conditions in a calendar year:

Control or process the personal data of at least one hundred thousand (100,000) consumers that are Indiana residents; or

Control or process the personal data of at least twenty-five thousand (25,000) Indiana consumers and derive more than fifty percent (50%) of their gross revenue from the sale of personal data.

Exemptions

The ICDPA exempts certain types of entities and data from its application. The following entities do not fall under the scope of the law:

The state, a state agency, or a body, authority, board, bureau, commission, district, or agency of any political subdivision of the state;

A third party under contract with an entity as described above;

Financial institutions or affiliates subject to Gramm-Leach-Bliley Act;

An entity subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA);

- A non-profit organization;
- Higher education institutions;
- Any public utility entity.

The law also does not have any application to the following types of data:

Medical data covered under any medical laws

Many forms of health information, records, data, and documents are protected and covered under HIPAA or other federal or state medical laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting protected under the federal Fair Credit Report Act (FCRA);

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

Exempt under ICDPA

Information originating from, indistinguishable from, or treated in the same manner as information that is exempt as per ICDPA;

Data used to protect human subjects

Identifiable private information used to protect human subjects under applicable laws or for formulating the related federal policy;

Emergency contact

Information used to contact an individual in an emergency; and

Employment-related data

Data processed or maintained:

- o 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;
- o that is necessary to retain to administer benefits for another individual relating to the individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party.

Obligations for Organizations Under ICDPA

Purpose Limitation

Under the ICDPA, a controller must limit all personal data collection to what is adequate, relevant, and reasonably necessary for the purposes for which the data is being collected.

The controller must seek the consumer's express consent for processing the personal data for a purpose that is not reasonably necessary or compatible with the purposes for which the data was originally collected.

Non-Discrimination

The controllers are barred from discriminating against the consumers for exercising their rights under the provisions of the ICDPA or processing their personal data in violation of state and federal laws prohibiting unlawful discrimination.

However, the law allows the controllers to offer different prices, rates, levels, quality, or selection of goods or services to a consumer if the consumer has exercised his/her right to opt out of the sale of personal data or the offer is based on the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Processing of Sensitive Personal Data

A data controller may only proceed with processing a consumer's sensitive personal data after acquiring that consumer's express consent. If the consumer is a known minor, any data processing must align with the relevant consent requirements in the federal Children's Online Privacy Protection Act (COPPA).

Privacy Notice

A controller must undertake all necessary and reasonable measures to provide consumers with an easily accessible, clear, and meaningful privacy notice that includes the following:

- Categories of personal data processed by the controller;
- Purposes of a controller's data processing activities;
- How consumers may exercise their data subject rights (DSRs);
- How consumers may appeal a controller's decision related to a consumer's request;
- Categories of third parties with whom the controller shares the personal data.

In case a controller sells consumers' personal data to third parties for targeted advertising purposes, the controller must disclose such arrangements clearly and conspicuously within the privacy notice as well as instructions on how consumers may exercise their right to opt out of such sales or use.

Additionally, the controller must establish and describe in the privacy notice at least one (1) or more safe and reliable means for consumers to exercise their data subject rights while taking into account the following:

- How consumers usually interact with the controller;
- The need for secure and reliable communication when dealing with such requests;
- The controller's ability to authenticate the identity of the individual exercising DSRs on their own or someone else's behalf.

Data Security Requirements

Appropriate to the volume and nature of the personal data, a controller must establish, implement, and maintain reasonable administrative, technical, and physical data security practices and measures that ensure the appropriate degree of protection for the confidentiality, integrity, and accessibility of all collected personal data.

Data Protection Impact Assessment

A controller is required to conduct and document a thorough data protection impact assessment (DPIA) for each of the following activities:

Processing of personal data for purposes of targeted advertising;

The sale of personal data;

Personal data processing activities carried out for profiling purposes if such profiling presents a reasonably foreseeable risk of:

- o unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- o financial, physical, or reputational injury to consumers;
- o a physical or another intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, if such intrusion would be offensive to a reasonable person; or
- o another substantial injury to consumers;

Processing of sensitive personal data;

Any personal data processing activity that poses a heightened risk of harm to consumers.

A single DPIA may be conducted to address a comparable set of processing operations that include similar activities. Moreover, an assessment carried out by the controller in pursuit of compliance with other regulations may also be used if the assessment has a reasonably comparable scope and effect to an assessment conducted under the ICDPA.

Disclosure of Pseudonymous Data or De-identified Data

With respect to the disclosure of de-identified or pseudonymous data, the controllers must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous or de-identified data is subject and to take appropriate steps to address any breaches of those contractual commitments.

Obligations of Processors

Assistance to Controller

The ICDPA requires the processors to assist the controllers by adopting appropriate technical and organizational measures to fulfill the controllers' obligations to respond to DSR requests and to meet security and breach notification obligations with respect to the personal data processed.

The processors must also assist the controllers by providing the necessary information to conduct DPIAs.

Processing under Contract

The processor shall be required to process the personal data on behalf of the controller in accordance with the terms of the contract between the controller and the processor (contract), setting forth the instruction for processing, nature, and purposes of the processing, the type of data processed, the duration of the processing and the rights and duties of both the parties. The contract shall also require the processor to:

Ensure the confidentiality of the personal data;

Delete or return the personal data to the collector on the direction of the controller, unless the law requires the retention of personal data;

Upon reasonable request from the controller, make available all the information in possession necessary to demonstrate compliance with its obligations;

Allow the controller to conduct an assessment, or arrange for a qualified and independent assessor to conduct an assessment, of the processor's policies and technical and organizational measures in support of the processor's obligations; and

Engage any subcontractor or agent through a written instrument requiring them to fulfill obligations towards the personal data.

Data Subject Rights

The ICDPA empowers consumers to have greater control over their personal data via DSRs. A consumer may invoke one or more data rights by submitting a request to a controller specifying which right they wish to invoke.

In the case of a child, their parent or legal guardian may invoke the right(s) on their behalf.

The data subject rights guaranteed by the ICDPA include the following:



Right to Access

All consumers have the right to confirm whether or not a data controller is processing their personal data and to access that data.



Right to Correction

All consumers have the right to correct any information that may have become inaccurate/obsolete/misleading since it was collected.



Right to Deletion

All consumers have the right to request the deletion of any personal data collected by or provided to a controller.



Right to Data Portability

All consumers have the right to obtain either a copy of or a representative summary of their personal data previously provided to the controller in a portable and readily usable format that allows the consumer to transmit the data or summary to any controller without any hindrance. The controller is under no obligation to fulfill requests to portable data by the same consumer for more than once in a twelve (12) month period. Further, the controller has the discretion to provide a copy of the data or a representative summary of the data depending upon the nature of the personal data.



Right to Opt-Out

All consumers have the right to opt out of the processing of their personal data for purposes of:

Targeted advertising;

Sale of personal data;

Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Response Period for DSR Requests

A controller is required to respond to any DSR request without undue delay but not later than forty-five (45) days after receiving the DSR request. This prescribed period may be extended by another forty-five (45) days when reasonably necessary, owing to the number of requests or the complexity of a particular request. However, the consumer must be informed of the delay as well as the reasons behind the delay.

Denial of a DSR Request

If a controller declines to take any action related to the consumer's request, it must inform the consumer of such denial within the forty-five (45) day period, along with a justification for declining to take action and appropriate instructions on how to appeal the decision.

A controller must establish an appropriate process for a consumer to appeal any decision made by the controller in relation to their DSR requests within a reasonable period. The process to launch appeals must be just as easily available as the process to submit a DSR request.

A controller must inform the consumer of any action taken or not taken as a result of their appeal within sixty (60) days of receiving their appeal. If the appeal is rejected, the controller is required to provide the consumer with information on how they may contact the Attorney General to launch a complaint.

Charges for DSR Requests

Any information provided to the consumers due to a DSR request must be provided free of charge once annually. A controller may charge a reasonable fee covering administrative costs if the requests are manifestly unfounded, excessive, or repetitive. However, the controller bears the burden of demonstrating that a particular request is manifestly unfounded, excessive, or repetitive.

If a controller cannot authenticate a DSR request via commercially reasonable efforts, they may decline to take action and may request additional information from the consumer to authenticate the request.

Regulatory Authority

The Office of the Attorney General of Indiana has the exclusive regulatory authority to enforce the provisions of the ICDPA. The Attorney General's powers and responsibilities include:

Initiating an action in the name of the state and seeking an injunction to restrain any violations of ICDPA as well as levying a civil penalty for each violation as prescribed by the law;

Recover reasonable expenses incurred in investigating and preparing the case, including attorney's fees;

Provide a controller or processor thirty (30) days written notice identifying the specific provisions of ICDPA that the Attorney General alleges have been or are being violated.

Within the third (30) days period, the Attorney General will not initiate any action against the controller or processor if the controller:

Cures the alleged violation; or

Provides the Attorney General with an express written statement stating that the violation has been

corrected and appropriate actions and measures have been taken to ensure no such violations occur in the future.

However, the Attorney General may initiate any legal action necessary if the controller or processor:

- Continue the alleged violation; or
- Commit breach of the express written statement provided to the attorney General.

Limitations

Limiting its scope of application, the ICDPA provides that it cannot restrict the ability of the controllers and the processors to do the following:

- Comply with federal, state, or local laws, rules, or regulations or implement and operate a facial recognition program approved by the Indiana gaming commission;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental authority;
- 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;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a product or service specifically requested by a consumer, perform a contract to which the consumer, or a parent of a child, is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer or parent before entering into a contract;
- Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual if the processing cannot be manifestly based on another legal basis;
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, investigate, report, or prosecute those responsible for any such action, and preserve the integrity or security of systems;
- Assist another controller, processor, or third party with any of their obligations per this regulation;
- Partake in scientific or statistical research in the public interest that follows all ethical guidelines and privacy regulations duly governed by an institutional review board that determines:
 - The information is likely to provide substantial benefits that do not exclusively accrue to the controller;

- o The expected benefits of the research outweigh the privacy risks;
- o The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

Further, ICDPA provides that any obligations placed on a controller or processor under its provisions do not prohibit or restrict a controller or a processor from collecting, maintaining, using, or storing data to:

- Conduct internal research to develop, improve, or repair products, services, or technology;
- Initiate a product recall;
- Identify and repair technical errors that impair existing or future functionalities;
- Perform internal operations that are:
 - o Reasonably compatible with the expectations of the consumer;
 - o Reasonably anticipated based on the consumer's existing relationship with the controller;
 - o Reasonably compatible with the product or service specifically requested by a consumer or parent of a child;
 - o Reasonably compatible with the performances of a contract of which the consumer is a part.

Further, ICDPA provides that any obligations placed on a controller or processor under its provisions do not prohibit or restrict a controller or a processor from collecting, maintaining, using, or storing data to:

- Conduct internal research to develop, improve, or repair products, services, or technology;
- Initiate a product recall;
- Identify and repair technical errors that impair existing or future functionalities;
- Perform internal operations that are:
 - o Reasonably compatible with the expectations of the consumer;
 - o Reasonably anticipated based on the consumer's existing relationship with the controller;
 - o Reasonably compatible with the product or service specifically requested by a consumer or parent of a child;
 - o Reasonably compatible with the performances of a contract of which the consumer is a part.

Similarly, any obligations placed on a controller or a processor under ICDPA do not apply if compliance with such a requirement would violate an evidentiary privilege under Indiana law.

Penalties For Non-Compliance

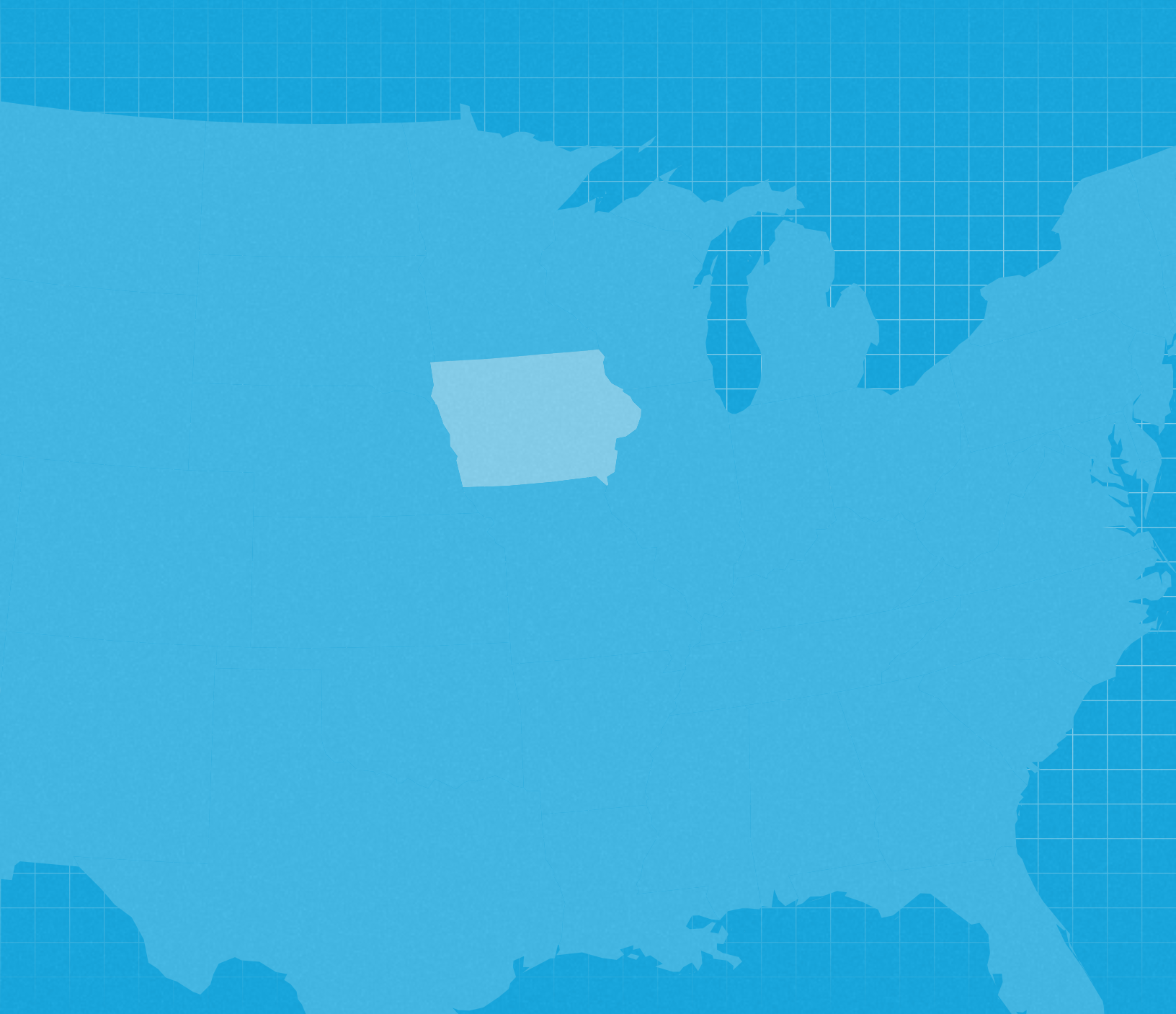
The ICDPA stipulates a civil penalty not exceeding seven thousand five hundred dollars (\$7,500) for every single violation of its provisions.

How an Organization Can Operationalize ICDPA

Here are some effective steps organizations can take to ensure their practices and daily operations are compliant with the law when it comes into effect:

- Develop formal policies and procedures for data collection (consent framework etc.) and processing, and update privacy policies as needed;
- Catalog their data inventories and classify sensitive personal data and personal data;
- Have a comprehensive data subject requests framework in place;
- Have technical and organizational security measures in place to protect personal data; and
- Conduct DPIAs, vendor assessments, and other risk assessments at regular intervals; and
- Ensure all the company's employees and staff are aware of their responsibilities under the law.

Iowa's Data Privacy Law



What is Iowa's Data Privacy Law - Senate File 262?

Iowa became the sixth state in the US to adopt a comprehensive data privacy law. Known as Senate File 262, the Iowa Senate and House unanimously passed the bill on March 15, 2023, before it was signed into law by Gov. Reynolds on March 28, 2023. The law shall go into effect on January 1, 2025.

Iowa's data privacy law joins five other US states and follows a format similar to California, Colorado, Connecticut, Utah, and Virginia state privacy laws. Due to its similarity to existing state laws, the law is not anticipated to impose significant compliance requirements on businesses already complying with pre-existing comprehensive state privacy regulations.

Who Needs to Comply with the Law

Material Scope

An entity conducting business in Iowa or producing products or services targeted to consumers who are Iowa residents shall be subject to the law if it meets the following requirements during a calendar year:

controls or processes the personal data of over 100,000 Iowa residents; or

controls or processes the personal data of over 25,000 Iowa residents and derives over 50% of its gross revenue from the sale of personal data.

Exemptions

The law exempts certain types of entities and data from its application. The following entities do not fall under the scope of the law:

Government entities;

Financial institutions, their affiliates, and entities subject to the Gramm-Leach-Bliley Act;

Entities who are subject to and comply with:

- o the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- o the Health Information Technology for Economic and Clinical Health Act (HITECH),

Non-profit organizations; and

Institutions of higher education.

The law also does not have any application to the following types of data:

Medical data covered under any medical laws

Many forms of health information, records, data, and documents are protected and covered under HIPAA or other federal or state medical laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting protected under the federal Fair Credit Report Act (FCRA);

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

COPPA data

Personal data used in accordance with the federal Children's Online Privacy Protection Act (COPPA);

Employment data

Personal data maintained for employment records.

Obligations for Organizations Under the Law

Security Measures

Based on the volume and nature of the personal data, the controllers are required to adopt and implement reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data.

Processing of Sensitive Data

The law obligates the controllers to present the consumers with a clear notice and an opportunity to opt-out in case of processing of sensitive data for a nonexempt purpose. For processing sensitive data belonging to a known child, the controllers must comply with the provisions of COPPA.

Non-Discrimination

The controllers are barred from discriminating against the consumers for exercising their rights under the law or processing their personal data violating state and federal laws prohibiting unlawful discrimination. However, the law allows the controllers to offer different prices, rates, levels, quality, or selection of goods or services to a consumer if the consumer has exercised his/her right to opt-out of the sale of personal data or the offer is based on the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Privacy Notice

The controllers are required to provide the consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the following:

- the categories of personal data processed by the controller;
- the purposes of personal data processing;
- the mechanism for exercising the rights under the law, including the right to appeal the denial of a consumer data request;
- the categories of personal data the controller shares with third parties, and
- the categories of third parties with whom the controller shares the personal data. In addition, if a controller sells a consumer's personal data to a third party or engages in targeted advertising, the controller must clearly disclose the activity to the consumer along with the mechanism through which the consumer may opt out of any such activity.

Disclosure of De-Identified or Pseudonymous Data

With respect to the disclosure of de-identified or pseudonymous data, the law requires the controllers to exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous or de-identified data is subject and to take appropriate steps to address any breaches of those contractual commitments.

Obligations of Processors

Assistance to Controller

The law requires the processor to assist the controller by adopting appropriate technical and organizational measures to fulfill the controller's obligations to respond to consumer data requests and meet security obligations concerning the personal data processed.

Processing under Contract

The processor shall be required to process the personal data on behalf of the controller in accordance with the terms of the contract between the controller and the processor (contract), setting forth the instruction for processing, nature, and purposes of the processing, the type of data processed, the duration of the processing and the rights and duties of both the parties. The contract shall also require the processor to:

ensure the confidentiality of the personal data;

delete or return the personal data to the collector on the direction of the controller unless the law requires the retention of personal data;

upon reasonable request from the controller, make available all the information in possession necessary to demonstrate compliance with its obligations; and

engage any subcontractor or agent through a written instrument requiring them to fulfill obligations towards the personal data.

Data Subject Rights

Under the law, the consumers may invoke the following rights by making an authenticated request (DSR) to the controller:



Right to Access

The consumer has a right to confirm whether the controller is processing his/her personal data and to access that data.



Right to Delete

The consumer has a right to get his/her personal data with the controller deleted.



Right to Data Portability

The consumer has a right to obtain a copy of his/her personal data.



Right to Opt-Out of the Sale

The consumer has a right to opt-out of the sale of his/her personal data.

With respect to the processing of personal data belonging to a child, a known child's parent or legal guardian may invoke such consumer rights on his/her behalf.

Response Period for DSRs

A controller must respond to a DSR without undue delay, but in all cases, within ninety (90) days from the receipt of the request. However, in cases where it is reasonably necessary, considering the complexity and number of the consumer's requests, the controller may seek an extension of another forty-five (45) days in the response period by informing the consumer of any such extension within the initial ninety-day response period along with the reason for an extension.

Denial of DSR

In case of a suspected fraudulent DSR, the controller may decline to take action by stating that the DSR could not be authenticated. In all other cases of denial to take action on a DSR, the controller must inform the consumer, without undue delay, about the justification for and instructions to appeal against such denial.

Charges for DSR

A consumer can make a DSR free of charge twice a year; however, where a DSR from a consumer is manifestly unfounded, excessive, repetitive, technically infeasible, or the controller reasonably believes that the primary purpose of the DSR is not to exercise a consumer right, it may charge the consumer a reasonable fee to cover the administrative costs of complying with the DSR or decline to act on the DSR. However, the controller shall bear the burden for demonstrating the unfounded, excessive, repetitive, and technically infeasible nature of a DSR.

Unauthenticated DSRs

The controller may decline to take action on a DSR that the controller is unable to authenticate using commercially reasonable efforts and may request the consumer to provide additional information reasonably necessary to authenticate the consumer and the DSR.

Appeal against Denial of DSR

A controller must establish a process, similar to the process for submission of DSR, for a consumer to file an appeal against the denial of DSR. The

controller is required to inform the consumer about the decision of the appeal within sixty (60) days from the receipt of the appeal and, in case the appeal is denied, provide the consumer with an online mechanism to submit a complaint with the attorney general.

Regulatory Authority

The Iowa attorney general has the exclusive authority to enforce the law. The attorney general is empowered to issue civil investigative demands to the controllers and processors and, in case the violations are not cured, to initiate a civil action.

Any Important Exemptions

The law provides certain exemptions for the controllers and processors concerning their processing of the consumers' personal data. These exemptions are as follows:

A controller or processor is not obligated under the law to:

- o re-identify de-identified data or pseudonymous data;
- o maintaining data in the identifiable form; or
- o collecting, obtaining, retaining, or accessing any data or technology in order to be capable of associating an authenticated consumer request with personal data.

A controller or processor is not obligated under the law to comply with a DSR, if:

- o the controller is not reasonably capable of associating the request with the personal data, or it would be unreasonably burdensome for the controller to associate the request with the personal data;
- o the controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, associate the personal data with other personal data about the same specific consumer; or
- o the controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor.

A controller is not obligated to fulfill a DSR with respect 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 organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Limitations

Limiting its scope of application, the law provides that it cannot restrict the ability of the controllers and the processors to do the following:

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;

investigate, establish, exercise, prepare for, or defend legal claims;

provide a product or service specifically requested by a consumer or parent or guardian of a child, perform a contract to which the consumer or parent or guardian of a child is a party, or take steps at the request of the consumer or parent or guardian of a child prior to entering into a contract;

take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person and where the processing cannot be manifestly based on another legal basis;

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;

engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entities that determine the following:

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

assist another controller, processor, or third party with any of the obligations under the law; or

provide personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

Further, the law provides that the obligations imposed on a controller or processor under its provisions shall not restrict a controller's or processor's 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 internal operations that are reasonably aligned with the expectations of the consumer or 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 parent or guardian of a child or the performance of a contract to which the consumer or parent or guardian of a child is a party.

However, it is pertinent to note that while processing personal data under any of the exemptions mentioned above, the controller must ensure the following:

the processing is reasonably necessary and proportionate to the exemption;

the processing is adequate, relevant, and limited to what is necessary in relation to the specific exemption; and

the personal data collected for such processing is subject to administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility.

Moreover, the law exempts the controllers and the processors from compliance with obligations under its provisions if such compliance violates an evidentiary privilege under the laws of the state of Iowa. The law also states that a controller or a processor shall not be in violation of the law if, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

The controllers and the processors are also exempt from fulfilling an obligation under the law if that adversely affects any other person's privacy, rights, or freedoms.

Penalties for Non-Compliance

The law does not prescribe any penalties for cases where the violation is cured by the controller or the processor within the ninety-day notice from the attorney general identifying the specific provisions of the

law being violated. However, in case of continuous violation or breach of an express written statement made regarding the cure of the violation, the attorney general may initiate an action in the name of the state and may seek an injunction to restrain any violations of the law and civil penalties of up to \$7,500 for each violation.

How an Organization Can Operationalize the Law

Organizations can operationalize Iowa's data privacy law by taking the following important steps:

Determine whether they meet the jurisdictional threshold of the law, including whether they hold personal data of Iowa residents and whether they meet the data volume threshold;

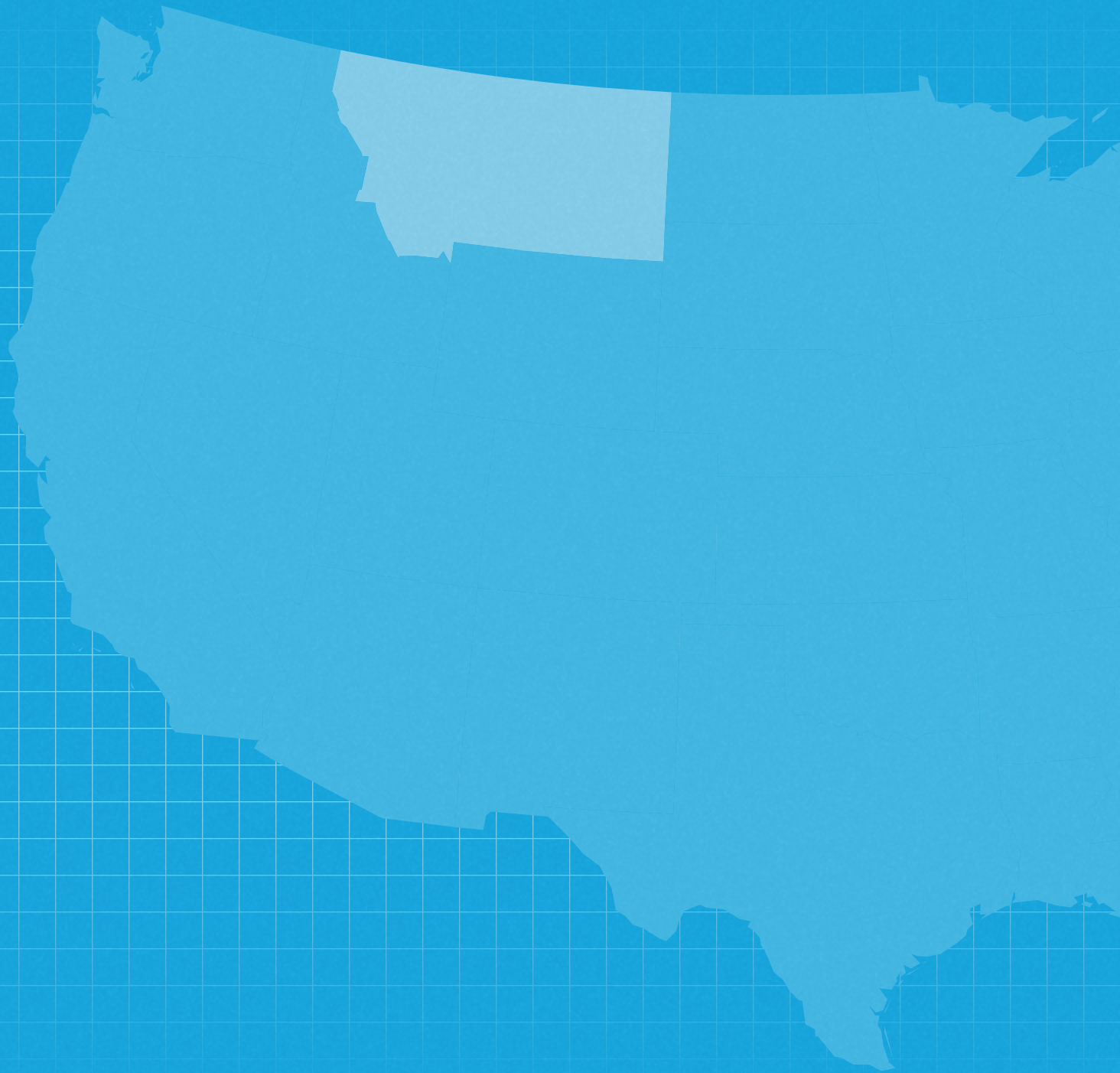
Determine their data inventories and classify data stores containing personal data of Iowa residents;

Develop clear and accessible privacy notice laying out consumers' rights and information about the processing of personal data;

Implement a robust framework for swiftly processing the DSRs as well as the consumer appeal against the denial of a DSR; and

Ensure personal data security by taking appropriate security measures.

Montana's Consumer Data Privacy Act



What is MCDPA?

In a growing effort to enact statewide data privacy laws, the Montana legislature unanimously approved the Montana Consumer Data Privacy Act (MCDPA) – Senate Bill 384 on April 21, 2023. Governor Greg Gianforte signed the bill into law on May 19, 2023.

The MCDPA stands out as the first data privacy law mandating controllers to give universal opt-out mechanisms in a state legislature with a Republican majority, and it is structured similarly to Connecticut's CTDPA. Organizations have until October 1, 2024, to abide by the law.

Who Needs to Comply with the MCDPA

Material Scope

The provisions of MCDPA apply to persons that conduct business in Montana or persons that produce products or services that are targeted to residents of Montana and:

- control or process the personal data of not less than 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

- control or process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

Exemptions

The MCDPA exempts the following entities from its application:

- body, authority, board, bureau, commission, district, agency or any political subdivision of the state of Montana;

- non-profit organization;

- institution of higher education;

- national securities association that is registered under the Federal Securities Exchange Act of 1934;

- financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, the Gramm-Leach-Bliley Act; or

- covered entity or business associate as defined in the privacy

regulations of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The law also does not have any application to the following types of data:

Medical data covered under any medical laws

Many forms of health information, records, data and documents protected and covered under HIPAA, or other federal or state medical/healthcare laws;

Personal data used for research

Identifiable private information collected, used or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting protected under the federal Fair Credit Report Act (FCRA);

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

COPPA data

Personal data used in accordance with the federal Children's Online Privacy Protection Act (COPPA);

ADA Data

Personal data collected, processed, sold, or disclosed in relation to price, route, or service by an air carrier subject to the Airline Deregulation Act of 1978 (ADA);

Employment data

Personal data maintained for employment records.

Obligations for Organizations Under MCDPA

Purpose Limitation

Under the MCDPA, a controller must limit all personal data collection to what is adequate, relevant, and reasonably necessary for the purposes for which the data is being collected.

Consent Requirements

A controller is required to provide an effective mechanism for consumers to revoke their consent for processing of personal data and on revocation of the consent, the controller must cease to process the personal data as soon as practicable, but not later than 45 days after the receipt of the request to revoke consent.

A controller must seek the consumer's express consent for processing the personal data for a purpose that is not reasonably necessary or compatible with the purposes for which the data was originally collected.

Non-Discrimination

A controller is barred from discriminating against the consumers for exercising their rights under the provisions of MCDPA or processing their personal data in violation of state and federal laws that prohibit unlawful discrimination. However, the law allows the controllers to offer different prices, rates, levels, quality, or selection of goods or services to a consumer if the consumer has exercised his/her right to opt-out of the sale of personal data or the offer is based on the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Privacy Notice Requirements

A controller is required to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the following:

the categories of personal data processed by the controller;

the purpose for processing personal data;

the categories of personal data that the controller shares with third parties, if any;

the categories of third parties, if any, with which the controller shares personal data;

an active e-mail address or other mechanisms that the consumer may use to contact the controller; and

how consumers may exercise their rights, including how they may appeal a controller's decision regarding the consumer's request.

Additionally, the controller must establish and describe in the privacy notice at least one (1) or more safe and reliable means for consumers to exercise their data subject rights (DSRs).

Security Requirements

The MCDPA requires organizations 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.

Data Protection Assessment

A data protection assessment (DPA) must be carried out and documented for each of the controller's processing activities that carry a heightened risk of harm to a customer, including:

the processing of personal data for the purposes of targeted advertising;

the sale of personal data;

the processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of:

- o unfair or deceptive treatment of or unlawful disparate impact on consumers;
- o financial, physical, or reputational injury to consumers;
- o a physical or other forms of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or
- o other substantial injuries to consumers; and

the processing of sensitive data.

A DPA must identify and balance potential benefits to the controller, the consumer, other stakeholders, and the public from the processing against any potential risks to the consumer's rights, as mitigated by any safeguards the controller may use to lessen these risks.

The controller must also consider the use of deidentified data, consumers' reasonable expectations, the context of the processing, and the relationship between the controller and the consumer whose personal data will be processed when conducting a DPA.

Moreover, an assessment carried out by the controller in pursuit of compliance with other regulations may also be used if the assessment has a reasonably comparable scope and effect to an assessment conducted under the MCDPA.

Any DPA that is relevant to an inquiry carried out by the attorney general may be requested to be disclosed by a controller, and the controller is required to make the assessment available to the attorney general.

Requirements for data protection assessments shall not be retroactive and must relate to processing operations started or generated after January 1, 2025.

De-Identified Data Requirements

Any controller in possession of de-identified data must:

- take reasonable measures to ensure that the de-identified data cannot be associated with an individual;
- publicly commit to maintaining and using de-identified data without attempting to re-identify the deidentified data; and
- contractually obligate any recipients of the de-identified data to comply with all provisions of the MCDPA.

A controller who discloses pseudonymous data or de-identified data must exercise reasonable oversight to ensure that any contractual obligations to which the pseudonymous data or de-identified data is subject are being met and must also take the appropriate steps if any of these obligations are violated.

Obligations of Processors

Assistance to Controller

The MCDPA requires the processors to assist the controllers by adopting appropriate technical and organizational measures to fulfill the controllers' obligations to respond to DSR requests and to meet security and breach notification obligations with respect to the personal data processed.

The processors must also assist the controllers by providing the necessary information to conduct DPAs.

Processing under Contract

The processor shall be required to process the personal data on behalf of the controller in accordance with the terms of the contract between the controller and the processor (contract), setting forth the instruction for processing, nature, and purposes of the processing, the type of data processed, the duration of the processing and the rights and duties of both the parties. The contract shall also require the processor to:

ensure the confidentiality of the personal data;

delete or return the personal data to the collector on the direction of the controller, unless retention of personal data is required by the law;

upon reasonable request from the controller, make available all the information in possession necessary to demonstrate compliance with its obligations;

allow the controller to conduct an assessment, or arrange for a qualified and independent assessor to conduct an assessment, of the processor's policies and technical and organizational measures in support of the processor's obligations; and

engage any subcontractor or agent through a written instrument requiring them to fulfill obligations towards the personal data.

Data Subject Rights

The following data privacy rights are afforded to consumers under MCDPA:



Right to Access

Consumers have the right to confirm that the data controller is processing their data and the right to access the data.



Right to Correction

Consumers have the right to correct any mistakes in their personal data.



Right to Deletion

Consumers have the right to delete any personal data that relates to them.



Right to Portability

Consumers have the right to obtain a copy of their data, in a portable format that is readily usable, allowing the consumers to transfer the data to another controller without any issues.



Right to Opt-Out

Consumers have a right to opt-out of the sale of their personal data or the processing of their personal data for the purposes of targeted advertising and behavioral profiling.

Right to Appeal

Controllers must establish a process for consumers to appeal the controller's refusal to act on a request within a reasonable period after the consumer's receipt of the decision.

Response Period of DSR Requests

Controllers have 45 days to respond to the DSR requests after receiving them. However, if reasonably necessary and depending on the volume and complexity of requests, the response time may be extended for an additional 45 days. In case of an extension in the response period, data controllers must inform consumers within the first 45 days.

Denial of a DSR Request

If a controller declines to take any action related to the consumer's request, it must inform the consumer of such denial within the forty-five (45) day period, along with a justification for declining to take action and appropriate instructions on how to appeal the decision.

A controller must establish an appropriate process for a consumer to appeal any decision made by the controller in relation to their DSR requests within a reasonable period. The process to launch appeals must be just as easily available as the process to submit a DSR request.

A controller must inform the consumer of any action taken or not taken as a result of their appeal within sixty (60) days of receiving their appeal. If the appeal is rejected, the controller is required to provide the consumer with information on how they may contact the Attorney General to launch a complaint.

Charges for DSR Requests

Any information provided to the consumers due to a DSR request must be provided free of charge once annually. A controller may charge a

reasonable fee covering administrative costs if the requests are manifestly unfounded, excessive, or repetitive. However, the controller bears the burden of demonstrating that a particular request is manifestly unfounded, excessive, or repetitive.

If a controller cannot authenticate a DSR request via commercially reasonable efforts, they may decline to take action and may request additional information from the consumer to authenticate the request.

Limitations

Limiting its scope of application, the MCDPA provides that it does not restrict the ability of the controllers and the processors to do the following:

- comply with federal, state, or municipal ordinances or regulations;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other government 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 municipal ordinances or regulations;
- investigate, establish, exercise, prepare for, or defend legal claims;
- provide a product or service specifically requested by a consumer;
- perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;
- take steps at the request of a consumer prior to entering a contract;
- take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis;
- 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, or investigate, report, or prosecute those responsible for any of these actions;
- engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines or similar independent oversight entities that determine:
- 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;

whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification.

assist another controller, processor, or third party with any of the obligations under the provisions of MCDPA; or

process personal data for reasons of public interest in public health, community health, or population health, but solely to the extent that the 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.

Further, MCDPA provides that any obligations placed on a controller or processor under its provisions do not prohibit or restrict a controller or a processor from collecting, maintaining, using, or storing 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 future functionalities;

Perform internal operations that are:

- o Reasonably aligned with the expectations of the consumer;
- o Reasonably anticipated based on the consumer's existing relationship with the controller;
- o Reasonably compatible with the product or service specifically requested by a consumer, or parent of a child;
- o Reasonably aligned with the performances of a contract to which the consumer is a party.

Similarly, any obligations placed on a controller or a processor under MCDPA do not apply if compliance with such a requirement would violate an evidentiary privilege under Montana law.

Regulatory Authority

The Office of the Attorney General of Montana is the exclusive regulatory authority for the enforcement of provisions of the MCDPA. The attorney general has the following responsibilities:

The controller must receive a notice of violation from the attorney general before any legal action is taken for a violation of any clause;

The attorney general may file a lawsuit if the controller doesn't fix the violation within 60 days of receiving the notice of violation;

No action must be taken against the controller if, within the 60-day window, the controller cures the observed violation and gives the attorney general an express written statement confirming that the alleged violations have been fixed and that no similar violations will occur in the future. This cure period, however, expires after April 1, 2026.

How an Organization Can Operationalize the MCDPA

Organizations can operationalize Montana's Consumer Data Privacy Act by:

Establishing policies and procedures for processing data;

Obtaining informed consent from consumers before collecting or sharing their data;

Implementing appropriate security measures such as data encryption, access controls, and audit logs to protect the confidentiality and integrity of the data;

Establishing a robust and comprehensive framework to receive and process DSR requests;

Conducting DPAs, vendor assessments, and other risk assessments at regular intervals;

Training employees who process consumer data;

Establishing the organization's policies and procedures that support compliance with evolving regulations and regularly monitor for any updates; and

Establishing a mechanism for handling any breaches of personal data or violations of the provisions of the MCDPA.

Oregon's Consumer Privacy Act



What is OCPA (Senate Bill 619)?

On June 22, 2023, the Oregon House of Representatives passed Senate Bill 619, also known as Oregon Consumer Privacy Act (OCPA), following an almost unanimous passage from the Senate on June 20, 2023. The Act's passage demonstrates wide bipartisan support for stronger privacy protections in the state of Oregon.

Modeled on Connecticut and Virginia data privacy laws, the OCPA must be signed by Governor Tina Kotek before it becomes law. Should it be approved, the law shall come into force on July 1, 2024.

Who Needs to Comply with OCPA

Material Scope

The law applies to any person that conducts business in Oregon, or that provides products or services to residents of Oregon, and during a calendar year, controls or processes:

the personal data of 100,000 or more consumers, other than personal data controlled or processed solely to complete a payment transaction; or

the personal data of 25,000 or more consumers while deriving 25 percent or more of the person's annual gross revenue from selling personal data.

Exemptions

The law exempts certain types of entities, data, and activities from its application.

Exempt Entities

The law also does not have any application to the following entities:

Public bodies/corporations;

Financial institutions, their affiliates, or their subsidiaries that are only and directly engaged in financial activities, as described in 12 U.S.C. 1843(k);

An insurer, as defined in ORS 731.106;

An insurance producer, as defined in ORS 731.104;

An insurance consultant, as defined in ORS 744.602;

A person that holds a third-party administrator license issued under ORS 744.710; and

A nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance.

Exempt Data

The law also does not have any application to the following types of data:

Data covered under medical laws

Protected health information processed in accordance with HIPAA, or other federal or state medical laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

GLBA data

Personal data collected, processed, sold, or disclosed in compliance with the Gramm-Leach-Bliley Act;

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

ADA data

Personal data collected, processed, sold, or disclosed in relation to price, route, or service under the Airline Deregulation Act (ADA), to the extent the provisions of OCPA are preempted by ADA; and

Employment data

Personal data maintained for employment records.

Exempt Activities

The law also does not have any application to the following activities:

Any activity that involves collecting, maintaining, disclosing, selling, communicating, or using information if done strictly in accordance with the provisions of the federal Fair Credit Report Act (FCRA) by:

- o A consumer reporting agency;
- o A person who furnishes information to a consumer reporting agency; or
- o A person who uses a consumer report.

The non-commercial activity of:

- o A publisher, editor, reporter, or other person who is connected with or employed by a newspaper, magazine, periodical, newsletter, pamphlet, report, or other publication in general circulation;
- o A radio or television station that holds a license issued by the Federal Communications Commission;
- o A nonprofit organization that provides programming to radio or television networks; or
- o An entity that provides an information service, including a press association or wire service.

Obligations for Organizations Under OCPA

Data Minimization and Purpose Limitation

Controllers must ensure transparency regarding their data collection activities and limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as initially disclosed to the consumer.

Consent Requirements

Controllers must provide consumers with an effective means to revoke their consent from having their personal information processed by the controller. The method must be at least as simple as the method used to obtain the consumer's consent. The controller must stop processing personal data as soon as possible when the consumer withdraws consent but no later than 15 days after receiving the revocation. A controller must not:

- process personal data without obtaining the consent of the data subject for purposes that are neither reasonably necessary nor compatible with those the controller specified;

process sensitive consumer data without the consumer's consent or, if the controller is aware that the consumer is a child, without following the Children's Online Privacy Protection Act's (COPPA) guidelines.

Targeted Advertising

A controller must not process a consumer's personal data for the purposes of targeted advertising, profiling the consumer to support decisions that have legal or significant consequences, or selling the consumer's personal data without the consumer's consent if the controller has actual knowledge that the consumer is at least 13 years old and not older than 15 years of age.

Privacy Notice Requirements

A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that:

outlines the categories of sensitive data, along with the types of personal data, that the controller processes;

specifies the reasons why the controller is processing the personal data;

explains how a consumer can exercise their rights, including how to appeal a controller's denial of a request made by a consumer;

specifies a list of all sensitive data categories, as well as all other categories of personal data, that the controller discloses with third parties;

specifies in sufficient detail each category of the third party that the controller shares personal data so that the consumer may determine the nature of each third party and, to the degree practicable, how each third party may process personal data;

provides consumers with the controller's email address or another online contact method that the controller actively reviews;

identifies the controller, including any assumed business name used in this state as well as any business name the controller registered with the Secretary of State;

provides a procedure by which the consumer may opt out of this type of processing;

describes any processing of personal data that the controller engages in for targeted advertising or to profile the consumer in support of decisions that have legal effects or effects of similar significance;

specifies the method(s) the controller has defined for receiving customer requests.

Security Requirements

To protect the confidentiality, integrity, and accessibility of personal data, the controller must establish, implement, and maintain the same safeguards described in ORS 646A.622 that are required to protect personal information, as defined in ORS 646A.602, to the extent necessary for the volume and nature of the data.

De-Identified Data Requirements

A controller that possesses de-identified data must:

Make reasonable efforts to ensure that the deidentified data cannot be used to identify a specific person;

Publicly commit to maintaining and using de-identified data without attempting to re-identify the deidentified data; and

Sign a contract with the recipient of the deidentified data, specifying that the recipient is responsible for complying with the controller's obligations.

A controller that discloses de-identified data must exercise reasonable oversight to ensure that any contractual obligations to which the deidentified data is subject are being followed, and they must take the necessary action to resolve any breaches of those obligations. This does not prohibit a controller from attempting to re-identify de-identified data solely to test the controller's methods for de-identifying data.

Data Protection Impact Assessment

A data protection assessment must be carried out and documented for each of the controller's processing operations that carry a heightened risk of harming a consumer. Processing activities that put consumers at heightened risk of harm include:

Processing personal data for the purpose of targeted advertising;

Processing sensitive data;

Selling personal data; and

Using the personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of:

- o Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- o Financial, physical, or reputational injury to consumers;
- o Physical or other types of intrusion upon a consumer's solitude, seclusion, or private affairs or concerns if the intrusion would be offensive to a reasonable person; or
- o Other substantial injuries to consumers.

A data protection assessment must identify and compare potential risks to consumers with how processing personal data may directly or indirectly benefit the controller, the consumer, other stakeholders, and the public while also considering the potential efficiency of the controller's security measures to reduce risks. The controller must conduct the assessment while considering the risks that de-identified data may help mitigate, consumers' reasonable expectations, the context in which the data is processed, and the relationship between the controller and the individuals whose personal data it will be processing.

Any data protection assessments that a controller has completed must be given to the Attorney General if those assessments are relevant to an investigation the Attorney General is conducting.

A controller can conduct a single data protection assessment to address a comparable set of processing operations that present a similar heightened risk of harm. Further, a data protection assessment conducted by the controller under any other law can also satisfy the requirements under the OCPA if the data protection assessment is reasonably similar in scope and effect to a data protection assessment conducted under OCPA.

Requirements for a data protection assessment are not retroactive and only apply to processing operations that start on or after July 1, 2024. A controller must keep all of their data protection assessments for at least five years. A data protection evaluation is private and cannot be disclosed.

Third-Party Processing Requirements

The controller must explain all categories of third parties—including sensitive data categories—with whom the controller shares personal data in sufficient detail for the consumer to understand the nature of each third party and, to the extent possible, how each third party may process personal data. Personal data should not be sold or otherwise voluntarily disclosed to a third party.

Non-Discrimination Requirements

A controller must not discriminate against a consumer who exercises a privilege provided to them by, for example, refusing to provide them with products or services, charging them a different price or rate, or offering them a different quality or variety of goods or services.

However, if a consumer voluntarily enrolls in a legitimate loyalty, rewards, premium features, discount, or club card program, the controller may make an offer to them for a different price, rate, level of quality, or selection of goods or services, including one for no fee or charge.

Data Processor Responsibilities

Assistance to Controller

A processor must comply with a controller's instructions and assist the controller in upholding its duties. In assisting the controller, the processor must:

- Enable the controller to respond to consumer requests by using methods that, to the extent reasonably practical, utilize appropriate technological and organizational measures, taking into consideration how the processor processes personal data and the information at its disposal;

- Implement reasonable administrative, technical, and physical security measures to ensure the security and privacy of the personal data the processor processes, taking into account how the processor uses the data and the information at its disposal;

- Provide the controller with information that is reasonably required to carry out and record data protection assessments.

Processing Under Contract

To process personal data on the controller's behalf, the processor and the controller must enter into a contract. The agreement must:

- Be valid and binding on both parties;

Clearly state how to process data, its nature and purpose, the categories of data that will be processed, and how long the processing will take;

Clearly state each party's obligations and rights concerning the contract's subject;

Ensure that each individual processing personal data is obligated to maintain the data's confidentiality;

Require that the processor deletes the personal data or return it to the controller upon request from the controller or completion of the services unless the processor is required by law to keep the data;

Require the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations of the processor;

Require the processor to enter into a subcontract with a person the processor engages to assist with processing personal data on the controller's behalf and, in the subcontract, requires the subcontractor to meet the processor's obligations under the processor's contract with the controller; and

Enable the controller, the controller's designee, or a qualified and independent person the processor engages in evaluating the processor's policies and organizational and technical measures for complying with its obligations in accordance with an appropriate and accepted control standard, framework, or procedure. Require the processor to cooperate with the assessment and report the assessment results to the controller upon the controller's request.

Data Subject Rights



Right to Know

Consumers have the right to obtain confirmation as to whether a controller is processing or has processed a consumer's personal data and the categories of personal data the controller is processing or has processed. Additionally, the controller must provide a consumer, at its option, with a list of the specific third parties—other than natural persons—to whom the controller has disclosed the consumer's personal data or any personal data.



Right to Correction

Consumers have the right to require a controller to correct inaccuracies in personal data about the consumer, taking into account the nature of the personal data and the controller's purpose for processing the personal data.



Right to Delete

Customers have the right to request that a controller delete any personal data about them, including data they gave to the controller directly, as well as the data the controller got from another source and derived data.



Right to Opt-Out

Consumers have the right to opt-out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes:

Targeted advertising;

Selling the personal data; or

Profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance.



Right to Data Portability

Consumers have the right to obtain a copy of their personal data processed by the controller in a portable and, to the degree technically possible, easily accessible format that enables hassle-free transmission of the personal data to another party.

How can consumers exercise their rights

Consumers have the right to exercise their rights at any time by making a request, through a method specified by the controller in its privacy notice, to a data controller and specifically highlighting the consumer rights they want to exercise. A parent or legal guardian of the child may exercise the child's consumer rights concerning the processing of personal data belonging to a known child. Similarly, a guardian or conservator may exercise the rights on behalf of a consumer that is subject to a guardianship, conservatorship, or other protective arrangement

Controller's response to data subject rights

A controller must respond to a consumer's request to exercise their rights without undue delay and no later than 45 days after receiving it. If the extension is considered to be reasonably necessary for meeting the

consumer's request, taking into account the complexity of the request and the frequency of requests the consumer makes, the controller may extend the time frame within which the controller responds by an additional 45 days. When extending the original 45-day response window, a controller must inform the consumer and provide a justification for the extension within the first 45 days after receiving the request.

If a controller chooses not to act on a consumer's request, the controller must inform the consumer without undue delay and no later than 45 days after receiving the request. The controller must include the justification for not taking action and also provide guidelines for appealing the controller's decision.

A controller is required to give consumers any data they want, just once for free every year. If a consumer makes a second or subsequent request within a year, the controller may do so with a reasonable fee to cover the administrative costs of doing so unless the purpose of the second or subsequent request is to confirm that the controller complied with the consumer's request to delete or correct inaccurate personal data. A controller must notify the consumer if the controller cannot, using commercially reasonable methods, authenticate the consumer's request without additional information from the consumer.

A controller is not required to authenticate an opt-out request; however, it may ask for additional information necessary to comply with the request, such as information necessary to identify the consumer requesting to opt-out. A controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that such a request is fraudulent. In such a case, the controller must notify the person who made such a request disclosing that such controller believes such request is fraudulent and the controller shall not comply with such request.

Appeal process

A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request. The controller's appeal process must:

- Give the consumer a reasonable amount of time to file an appeal after receiving the controller's denial;
- Be readily accessible to consumers;
- Appear and be equivalent to how a consumer must submit a request; and

Require the controller to inform the consumer in writing of their decision and the reasons behind it within 45 days of receiving the appeal, whether they approved it or denied it. The notice must include or define information enabling the consumer to contact the Attorney General and file a complaint if the controller denies the appeal.

Regulatory Authority

The Oregon Attorney General has the exclusive authority to enforce the provisions of OCPA.

Limitations

The provisions of OCPA do not restrict a controller or a processor from doing the following:

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;

Investigate, establish, initiate, or defend legal claims;

Prevent, detect, protect against, or respond to, and investigate, report, or prosecute persons responsible for security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity, or preserve the integrity of systems;

Identify and repair technical errors in a controller's or processor's information systems that impair existing or intended functionality;

Provide a product/service specifically requested by a consumer, the parent or guardian of a child on the child's behalf, or as the guardian or conservator of a person subject to a guardianship, conservatorship, or other protective arrangement on the person's behalf;

Negotiate, enter into or perform a contract with a consumer, including fulfilling the terms of a written warranty;

Protect any person's health and safety;

Effectuate a product recall;

Conduct internal research to develop, improve or repair products, services or technology;

Perform internal operations that are reasonably aligned with a consumer's expectations, that the consumer may reasonably anticipate based on the consumer's existing relationship with the controller or that are otherwise compatible with processing data for the purpose of providing a product or service the consumer specifically requested or for the purpose of performing a contract to which the consumer is a party; or

Assisting another controller or processor with any of the activities listed above.

Any obligation placed on a controller or a processor under OCPA does not apply if compliance by the controller or processor would violate an evidentiary privilege under Oregon laws.

Penalties for Non-Compliance

For each infraction, the Attorney General can seek a civil penalty of up to \$7,500. If the Attorney General determines the controller can correct the violation, the controller must be notified of the violation before the Attorney General may initiate an action. The Attorney General may file a lawsuit without additional notice if the controller doesn't correct the infraction within 30 days after receiving notice of it.

The Attorney General shall bring an action within five years after the date of the last act of a controller that constituted the violation for which the Attorney General seeks relief.

How an Organization Can Operationalize the OCPA

Organizations can operationalize Oregon Consumer Privacy Act (OCPA) by:

Establishing policies and procedures for processing data in compliance with the requirements of the OCPA;

Developing clear and accessible privacy notices in compliance with the requirements of the OCPA;

Obtaining informed consent from individuals before processing their sensitive personal data;

Developing a robust framework for receiving and processing data requests and complaints from consumers;

Ensuring personal data security by taking appropriate security measures; and

Training employees who handle the consumers' data on the organization's policies and procedures, as well as the requirements of the OCPA.

Texas Data Privacy and Security Act



What is TDPSA?

On May 28, 2023, the Texas legislature passed the Texas Data Privacy and Security Act (TDPSA), also known as H.B. 4, making Texas the tenth US state to pass a comprehensive data privacy law. The TDPSA and Virginia's Consumer Data Protection Act (VCDPA) share several similarities, although some distinctions exist. Governor Abbott signed the TDPSA into law on June 18, 2023, and will take effect on July 1, 2024.

With the passage of TDPSA, Texas became the fifth state to pass comprehensive data privacy legislation in 2023, the other four being Iowa, Montana, Tennessee, Indiana, and Nevada.

Who Needs to Comply with TDPSA

Material Scope

The TDPSA applies only to persons who:

- conduct business in Texas or produce products or services consumed by Texas residents;
- process or engage in the sale of personal data; and
- are not small businesses as defined by the United States Small Business Administration (SBA), i.e., an independent business having fewer than 500 employees.

Exemptions

The TDPSA does not apply to:

- a state agency or a political subdivision of Texas;
- a financial institution or data subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);
- the processing of personal data by a person during a purely personal or household activity;
- a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services (HHS), established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH);
- a nonprofit organization;

an institution of higher education; and

an electric utility, a power generation company, or a retail electric provider.

The following information is also exempt from the application of the TDPSA:

Medical data covered under any medical laws

Many forms of health information, records, data, and documents protected and covered under HIPAA or other federal or state medical/healthcare laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting to the extent the activity is authorized and regulated by the federal Fair Credit Report Act (FCRA);

GLBA data

Financial data subject to Title V of the federal Gramm-Leach-Bliley Act;

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

Employment data

Personal data maintained for employment records.

Obligations for Organizations Under TDPSA

Data Minimisation and Purpose Limitation

Controllers must ensure transparency regarding their data collection activities and limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as initially disclosed to the consumer.

Security Measures

Controllers must also establish, implement, and maintain acceptable administrative, technical, and physical data security procedures that are appropriate to the volume and nature of the personal data at stake to safeguard the privacy, accuracy, and accessibility of personal data.

Non-Discrimination

Controllers are barred from discriminating against consumers for exercising their rights under the provisions of TDPSA or processing their personal data in violation of state and federal laws prohibiting unlawful discrimination. However, the law allows the controllers to offer different prices, rates, levels, quality, or selection of goods or services to a consumer if the consumer has exercised his/her right to opt out of the sale of personal data or the offer is based on the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Methods for Submission of DSR Requests

Controllers must establish two or more secure and reliable methods to enable the consumers to submit a request to exercise their consumer rights under the TDPSA. Such methods must take into account the following:

- the ways in which the consumers normally interact with the controller;
- the necessity for secure and reliable communications of those requests; and
- the ability of the controller to authenticate the identity of the consumer making the request.

Consent Requirements

Controllers must not process a consumer's personal data for a purpose that is neither reasonably necessary nor compatible with the disclosed purpose for which the personal data is processed unless the controller obtains the consumer's consent.

Further, a controller must not process sensitive data concerning a consumer without obtaining the consumer’s consent. In the case of the processing of sensitive data concerning a known child, the controller must process the data in accordance with the federal Children’s Online Privacy Protection Act (COPPA).

Universal Opt-Out Mechanism Requirements

As of January 1, 2025, the TDPSA will require that controllers establish global opt-out mechanisms, such as the Global Privacy Control (“GPC”), to allow consumers to refuse the sale of their personal information and targeted advertising.

Privacy Notice Requirements

A controller must provide consumers with a reasonably accessible and clear privacy notice that includes the following:

- the categories of personal data that the controller processes, including, if relevant, any sensitive data that the controller processes;
- the purpose of processing personal data;
- how consumers can exercise their consumer rights, including the procedure for appealing a controller’s decision about a consumer’s request;
- the categories of personal data, if any, that the controller shares with third parties;
- the categories of third parties, if any, that the controller shares personal data with; and
- a description of the procedures for submitting consumer rights requests.

When engaging in the sale of sensitive personal data

A controller must include the following notice in the same location and in the same manner as the privacy notice:

NOTICE: We may sell your sensitive personal data.

When engaging in the sale of biometric data

A controller must include the following notice in the same location and in the same manner as the privacy notice:

NOTICE: We may sell your biometric personal data.

De-Identified or Pseudonymous Data Requirements

A controller in possession of de-identified data must:

- make reasonable efforts to ensure that the data cannot be associated with an individual;
- publicly commit to maintaining and using de-identified data without attempting to re-identify it;
- contractually obligate any recipient of the de-identified data to comply with the provisions of the TDPSA.

Data Protection Impact Assessment

A controller must conduct and document a data protection assessment (DPA) of each of the following processing activities involving personal data:

- Processing personal data for the purposes of targeted advertising;
- Selling personal data;
- Processing personal data to profile consumers if the profiling presents a reasonably foreseeable risk of:
 - o Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
 - o Financial, physical, or reputational injury to consumers;
 - o Physical or other intrusions upon the solitude or seclusion, or the private affairs or concerns, of consumers; or
 - o Other substantial injuries to consumers;
 - o Processing sensitive data; and
 - o Any other processing of personal data that presents a heightened risk of harm to consumers.

A DPA must identify and weigh any potential direct or indirect benefits to the controller, the consumer, other stakeholders, and the public from the processing against any potential risks to the consumer's rights, as mitigated by the controller's use of safeguards that reduce the risks.

A DPA carried out by the controller to comply with other regulations may also be used for the purposes of TDPSA if the DPA has a reasonably comparable scope and effect to a DPA conducted under the provisions of TDPSA.

Data Processor Responsibilities

Assistance to Controller

A processor must comply with a controller's instructions and assist the controller in fulfilling their obligations, including:

- assisting the controller in responding to consumer rights requests;
- considering the nature of processing and the information at the processor's disposal, support the controller in complying with the obligation relating to the security of processing personal data and the notification of a system security breach; and
- providing the information required for the controller to carry out and record data protection assessments.

Processing under Contract

The processor shall be required to process the personal data on behalf of the controller in accordance with the terms of the contract between the controller and the processor. The contract must include the following:

- clear instructions for processing data;
- the nature and purpose of processing data;
- the type of data subject to processing;
- the duration of the processing;
- the rights and obligations of both the parties; and
- o a requirement that the processor shall:
 - o ensure the confidentiality of the personal data;

- o delete or return the personal data to the collector on the direction of the controller unless retention of personal data is required by the law;
- o upon reasonable request from the controller, make available all the information in possession necessary to demonstrate compliance with its obligations;
- o allow the controller to conduct an assessment, or arrange for a qualified and independent assessor to conduct an assessment, of the processor's policies and technical and organizational measures in support of the processor's obligations; and
- o engage any subcontractor or agent through a written instrument requiring them to fulfill obligations towards the personal data.

Data Subject Rights

The TDPSA grants consumers the following rights:



Right to Confirm

The right to confirm whether a controller is processing a consumer's personal data.



Right to Access

The right to access personal data that is being processed.



Right to Correct Inaccuracies

The right to correct any inaccuracies in consumers' personal data.



Right to Delete

The right to delete personal data provided by or obtained about the consumer.



Right to Obtain a Personal Copy

The right to obtain a portable copy of the consumer's personal data.



Right to Opt-Out

The right to opt-out of processing of personal data for purposes of:

targeted advertising (defined as displaying to a consumer an advertisement that is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests);

the sale of personal data; or

profiling (defined as any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements).

How can consumers exercise their rights

Consumers have the right to exercise their rights at any time by making a request to a data controller and specifically highlighting the consumer rights they want to exercise. A parent or legal guardian of the child may exercise the child's consumer rights concerning the processing of personal data belonging to a known child.

Controller's response to data subject rights

A controller must comply with a request made by a consumer to exercise their rights unless an exemption applies. A controller must respond to a consumer's request without undue delay and no later than 45 days from the day the request was received. However, when it is deemed reasonably necessary, taking into account the complexity and volume of the customer's requests, the controller may extend the response period once by an additional 45 days. However, the controller must notify the consumer of the extension within the first 45 days of the response period, along with the reason for the extension.

A controller is required to respond to a consumer request for information without charge at least twice a year for each consumer. Consumers may be charged a reasonable fee to offset the administrative costs of complying with requests that are clearly unjustified, excessive, or recurrent, or the controller may choose not to act on the request altogether. However, the controller must prove that a request is manifestly unfounded, excessive, or repetitive.

A controller is not required to comply with a consumer request submitted if the controller cannot authenticate the request using commercially reasonable efforts. Instead, the controller may request that the consumer

provide any additional information reasonably required to authenticate the consumer and the consumer's request.

Lastly, if the controller has obtained the personal data about a consumer from a source other than the consumer, the controller is considered in compliance with the consumer's request for deletion of personal data if the controller:

retains a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using the retained data for any other purpose; and opts the consumer out of the processing of that personal data for any purposes other than a purpose that is exempt under the provisions of the TDPSA.

Appeal process

A controller must set up a procedure for the consumer to appeal the controller's denial of a request within a reasonable amount of time after receiving the decision. The appeal procedure must be clearly available and similar to the procedure for requesting action to exercise consumer rights. A controller must provide written notice to the consumer of any action taken or not taken in response to an appeal no later than 60 days after the date the appeal was received. This notice must include a documented justification for the decision. The online method for contacting the Attorney General to file a complaint must be made available to the consumer if the controller rejects an appeal.

Regulatory Authority

The Texas Attorney General has the exclusive authority to enforce the provisions of the TDPSA. The attorney general has the right to issue a civil investigative demand if there is reason to believe an individual has violated the TDSPA or is doing so.

The attorney general must issue a 30-day notice of violation to a person before bringing any enforcement action for any violation of the law. The attorney general must not bring an action against the person if:

- within the 30-day period, the person cures the identified violations;
- the person provides the attorney general a written statement that the person:
 - o cured the alleged violation;

- o notified the consumer that the consumer’s privacy violation was addressed if the consumer’s contact information had been made available to the person;
- o provided supportive documentation to show how the privacy violation was cured; and
- o made changes to the internal policies, if necessary, to ensure that no such further violations will occur.

Limitations

The obligations imposed under TDPSA do not restrict a controller’s or a 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;

Investigate, establish, exercise, prepare for, or defend legal claims;

Provide a product/service specifically requested by a consumer, perform a contract, fulfill the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another natural person;

Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity;

Preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action;

Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines if:

- o Deletion of the information is likely to provide substantial benefits to the controller;
- o The expected benefits of the research outweigh the privacy risks;
- o The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification; and

Assist another controller, processor, or third party with their obligations under TDPSA.

Nothing under TDPSA may restrict a controller or processor's ability to collect, use, or retain data to:

- Conduct internal research to develop, improve, or repair products, services, or technology;
- Initiate a product recall;
- Identify and repair technical errors that impair existing or intended functionality; or
- Perform internal operations that are reasonably aligned with the consumer's expectations or 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.

Similarly, any obligations placed on a controller or a processor under TDPSA do not apply if:

- compliance by the controller or processor would violate an evidentiary privilege under Texas law or adversely affect the rights or freedoms of a person; and
- compliance by the controller, processor, or third party requires them to disclose a trade secret.

Penalties for Non-Compliance

A person who violates any provision of the TDPSA and fails to cure that within the 30-day cure period or who breaches a written statement provided to the attorney general pursuant to notice of violation is liable for a civil penalty in an amount not to exceed \$7,500 for each violation.

How an Organization Can Operationalize the TDPSA

Organizations can operationalize the Texas Data Privacy and Security Act (TDPSA) by:

- Establishing policies and procedures for processing data in compliance with the requirements of the TDPSA;
- Developing clear and accessible privacy notices in compliance with the requirements of the TDPSA;
- Obtaining informed consent from individuals before processing their sensitive personal data;

Developing a robust framework for receiving and processing data requests and complaints from consumers;
and

Train employees who handle the consumers' data on the organization's policies and procedures, as well as the requirements of the TDPSA.

Tennessee Information Protection Act



What is TIPA?

The Tennessee Information Protection Act (TIPA) received unanimous support in both houses of the State General Assembly, with Governor Bill Lee signing it into law on May 11, 2023.

The Tennessee Information Protection Act (TIPA) contains several provisions that have become a staple of state data privacy laws within the US. However, there are instances where TIPA stands apart from some of its sister data privacy regulations owing to its emphasis on ensuring an affirmative defense for organizations that demonstrate a willingness to inculcate strict data privacy measures via the National Institute of Standards and Technology (NIST) privacy framework.

The Tennessee Information Protection Act (TIPA) will come into effect on July 1, 2024.

Who Needs to Comply with the Law

Material Scope

The law applies to persons that conduct business in Tennessee or produce products or services that are targeted to residents of Tennessee and that:

Control or process the personal information of at least one hundred thousand (100,000) consumers during a calendar year;

Control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information.

Exemptions

The TIPA exempts the following entities from its application:

A body, authority, board, bureau, commission, district, or agency of Tennessee or of a political subdivision of Tennessee;

A financial institution, an affiliate of a financial institution subject to Title V of the federal Gramm-Leach-Bliley Act;

An individual, firm, association, corporation, or other entity that is licensed in Tennessee as an insurance company and transacts insurance business;

A covered entity or business associate governed by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the federal Health Information Technology for Economic and Clinical Health Act (HITECH);

A non-profit organization; and

An institution of higher education.

The law also does not have any application to the following types of data:

Medical data covered under any medical laws

Many forms of health information, records, data, and documents are protected and covered under HIPAA or other federal or state medical/healthcare laws;

Personal data used for research

Identifiable private information collected, used, or shared in research conducted in accordance with applicable laws;

FCRA-covered data

Any personal information of consumers collected or used for consumer credit scoring and reporting to the extent the activity is authorized and regulated by the federal Fair Credit Report Act (FCRA);

GLBA data

Financial data subject to Title V of the federal Gramm-Leach-Bliley Act;

Driver data

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

FERPA data

Personal data is regulated by the federal Family Educational Rights and Privacy Act (FERPA);

FCA data

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (FCA);

Employment data

Personal data is maintained for employment records.

Obligations for Organizations Under the TIPA

Purpose Limitation

Under TIPA, a controller must limit the collection of personal information to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed. Further, the controller must not process personal information for purposes that are beyond what is reasonably necessary to and compatible with the disclosed purposes unless the controller obtains the consumer's consent.

Security Measures

TIPA requires the controllers to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal information. The data security practices must be appropriate to the volume and nature of the personal information at issue.

Non-discrimination

A controller is barred from discriminating against the consumers for exercising their rights under the provisions of TIPA or processing their personal data in violation of state and federal laws that prohibit unlawful discrimination. However, the law allows the controllers to offer different prices, rates, levels, quality, or selection of goods or services to a consumer if the consumer has exercised his/her right to opt out of the sale of personal data or the offer is based on the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Consent Requirements

Under the provisions of TIPA, a controller must not process sensitive data concerning a consumer without obtaining the consumer's consent. In the case of the processing of sensitive data concerning a known child, the controller must process the data in accordance with the federal Children's Online Privacy Protection Act.

Further, a controller must seek the consumer's express consent for processing the personal data for a purpose that is not reasonably necessary or compatible with the purposes for which the data was originally collected.

Privacy Notice Requirements

Upon receipt of an authenticated consumer request, a controller must provide the consumer with a reasonably accessible, clear, and meaningful privacy notice that includes

The categories of personal information processed by the controller;

The purpose for processing personal information;

How consumers may exercise their consumer rights under TIPA, including how a consumer may appeal a controller's decision with regard to the consumer's request;

The categories of personal information that the controller sells to third parties, if any;

The categories of third parties, if any, to whom the controller sells personal information; and

The right to opt out of the sale of personal information to third parties and the ability to request deletion or correction of certain personal information.

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

Methods for Submission of DSR Requests

A controller must provide and describe in the privacy notice at least one of the following methods for consumers to submit a request to exercise consumer rights under this part:

A toll-free telephone number;

An email address;

A web form; or

A clear and conspicuous link on the controller's main internet homepage to an internet webpage enables a consumer to exercise the rights provided under TIPA.

Regardless of the method, the controller must ensure the method is capable of authenticating the identity of the consumer making the request. The controller must not require a consumer to create a new account in order to exercise consumer rights under TIPA but may require a consumer to use an existing account.

Data Protection Assessment

A controller must conduct and document a data protection assessment (DPA) of each of the following processing activities involving personal information:

Processing of personal information for purposes of targeted advertising;

Sale of personal information;

Processing of personal information for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

- o Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- o Financial, physical, or reputational injury to consumers;
- o Physical or other intrusions upon the solitude or seclusion, or the private affairs or concerns, of consumers;
- o Other substantial injuries to consumers;

Processing of sensitive data;

Processing activities that involve personal information pose a potential risk of harm to consumers.

A DPA must appropriately identify the benefits resulting, directly and indirectly, from the processing activities to the data controller, consumer, and other stakeholders such as the public and should also identify relevant risks that may arise to the rights of consumers provided under TIPA, that the safeguards employed by the controller may reduce. While conducting a DPA, the controller must also consider the use of de-identified data, the expectations of consumers, and the context of the data processing activities.

The Attorney General and Reporter may request any data controller to disclose a DPA that is relevant to an investigation. The Attorney General and Reporter may also use a DPA to evaluate a controller's compliance with their responsibilities under TIPA.

Furthermore, the controllers may conduct a single DPA to address comparable processing operations that include similar activities. Moreover, a DPA carried out by the controller to comply with other

regulations may also be used for the purposes of TIPA if the DPA has a reasonably comparable scope and effect to a DPA conducted under the provisions of TIPA.

Requirements for DPAs are not retroactive and are only applicable to processing operations created or generated on or after July 1, 2024.

Processing De-Identified Data

A controller in possession of de-identified data must:

- Take reasonable measures to ensure that the data cannot be associated with a natural person;
- Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and
- Contractually obligate recipients of the de-identified data to comply with the requirements (a) and (b) above.

Privacy Program

Under the provisions of TIPA, a controller or processor must create, maintain, and comply with a written privacy program that reasonably conforms to the National Institute of Standards and Technology (NIST) privacy framework entitled “A Tool for Improving Privacy through Enterprise Risk Management Version 1.0.”

In case of a subsequent revision to the NIST privacy framework, a controller or processor must reasonably conform its privacy program to the revised framework not later than one (1) year after the publication date stated in the most recent revision.

The scale and scope of a controller or processor’s privacy program are appropriate if it is based on all of the following factors:

- The size and complexity of the controller or processor’s business;
- The nature and scope of the activities of the controller or processor;
- The sensitivity of the personal information processed;
- The cost and availability of tools to improve privacy protections and data governance; and
- Compliance with a comparable state or federal law.

A controller or processor's privacy program must also disclose the commercial purposes for which the controller or processor collects, controls, or processes personal information.

In addition to a privacy program, a controller may be certified pursuant to the Asia Pacific Economic Cooperation's Cross Border Privacy Rules System. A processor may be certified pursuant to the Asia Pacific Economic Cooperation's Privacy Recognition for Processors system.

Lastly, a controller or processor, who creates, maintains, and complies with a written privacy program, has an affirmative defense to a cause of action for a violation of the provisions of TIPA.

Data Processor Responsibilities

Assistance to Controller

The TIPA requires the processors to assist the controllers by adopting appropriate technical and organizational measures to fulfill the controllers' obligations to respond to DSR requests and provide the necessary information to conduct DPAs.

Processing Under Contract

The processor shall be required to process the personal data on behalf of the controller in accordance with the terms of the contract between the controller and the processor (contract), setting forth the instruction for processing, nature, and purposes of the processing, the type of data processed, the duration of the processing and the rights and duties of both the parties. The contract shall also require the processor to:

- ensure the confidentiality of the personal data;

- delete or return the personal data to the collector on the direction of the controller unless the law requires the retention of personal data;

- upon reasonable request from the controller, make available all the information in possession necessary to demonstrate compliance with its obligations;

- allow the controller to conduct an assessment, or arrange for a qualified and independent assessor to conduct an assessment, of the processor's policies and technical and organizational measures in support of the processor's obligations; and

- engage any subcontractor or agent through a written instrument requiring them to fulfill obligations towards the personal data.

Data Subject Rights

The following data rights are afforded to consumers under TIPA:



Right to Access

Consumers have the right to confirm whether a controller is processing their personal information and access it.



Right to Correction

Consumers have the right to correct inaccuracies in their personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.



Right to Deletion

Consumers have the right to delete personal information provided by or obtained about them. However, this right does not extend to de-identified data, provided that such data is not linked to a specific consumer.



Right to Portability

Consumers have the right to request a copy of the 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 hindrance, where the processing is carried out by automated means.



Right to Disclosure

Consumers have the right to request a controller that has sold or shared their personal information with third parties to disclose the following:

Categories of personal information sold;

Categories of third parties to which the personal information was sold by category of personal information for each category of third parties to which the personal information was sold;

Categories of personal information about the consumer that the business disclosed for a business purpose.



Right to Opt-Out

Consumers have the right to opt-out of the sale of their personal information.

Response Period of DSR Requests

A controller must respond to all DSR requests within forty-five (45) days after receiving them. A further extension of forty-five (45) days is possible when reasonably necessary, considering the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial forty-five (45) days period.

Denial of DSR Requests

In case the controller declines to take action related to a consumer's request, it must inform the consumer of such denial without undue delay and within forty-five (45) days of receiving the request, in addition to the justification for declining to take action and detailed instructions on how consumers may appeal the decision.

The process established for the consumer to appeal the controller's refusal to take action must be available in a conspicuous manner, without causing additional cost to the consumer, while also being similar to the process of making other consumer requests. The controller must inform the consumer of any action taken or not taken concerning their appeal within sixty (60) days of receiving the appeal, alongside a written explanation of the reasons behind the decision. If the appeal is denied, the controller shall ensure they communicate an online mechanism to the consumer allowing them to contact the Attorney General's office to submit an official complaint.

Charges for DSR Request Fulfillment

Any information provided to the consumer as a result of a DSR request must be provided free of charge twice annually per consumer. If a DSR request is manifestly unfounded, technically infeasible, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. However, the burden of proof of demonstrating the manifestly unfounded, technically infeasible, excessive, or repetitive nature of the request rests on the controller.

If the controller cannot authenticate a DSR request via commercially reasonable efforts, they may decline to take action and seek additional information reasonably necessary from the consumer to authenticate the request.

Regulatory Authority

The Tennessee Attorney General & Reporter (AGR) has the exclusive authority to enforce the provisions of TIPA.

The AGR may develop reasonable cause to believe that a controller or processor is in violation of this part based on the AGR's own inquiry or on consumer or public complaints and may issue a civil investigative demand. However, prior to initiating any action, the AGR must provide a controller or processor sixty days' written notice identifying the specific provisions of TIPA that the AGR alleges have been violated. If, within the sixty-day period, the controller or processor cures the noticed violation and provides the AGR an express written statement that the alleged violations have been cured and that no further violations shall occur, then the AGR shall not initiate an action against the controller or processor.

However, if the controller or processor continues their violation following the remedy period or if it violates any of the claims made in the written statement, then the AGR may bring an action in a court of law seeking any of the following relief:

- A declaratory judgment that the act or practice violates TIPA;
- Injunctive relief, including preliminary and permanent injunctions;
- Civil penalties;
- Reasonable attorney's fees and investigative costs;
- Other relief the court determines to be appropriate.

Limitations

The UCPA contains important substantive exemptions, including:

- 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 believes may violate federal, state, or local laws, rules, or regulations;
- Investigate, establish, exercise, prepare for, or defend legal claims;
- Provide a product/service specifically requested by a consumer, perform a contract, fulfill the terms of a written warranty, or take steps at the request of the consumer before entering into a contract;

Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another natural person;

Assist another controller, processor, or third party with their obligations under TIPA;

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

Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines if:

Deletion of the information is likely to provide substantial benefits to the controller;

The expected benefits of the research outweigh the privacy risks;

The controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with reidentification.

Nothing under TIPA may restrict a controller or processor's ability to collect, use, or retain data to:

Conduct internal research to develop, improve, or repair products, services, or technology;

Initiate a product recall;

Identify and repair technical errors that impair existing or intended functionality; or

Perform internal operations that are reasonably aligned with the consumer's expectations or 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.

Similarly, any obligations placed on a controller or a processor under TIPA do not apply:

If compliance by the controller or processor would violate an evidentiary privilege under Tennessee law or adversely affect the rights or freedoms of a person;

To the processing of personal information by a person in the course of a purely personal activity.

Penalties for Non-Compliance

A court may impose a civil penalty of up to fifteen thousand dollars (\$15,000) for each violation of the provisions of TIPA that must be assessed per the following criteria:

- Each provision of TIPA is a separate violation; and
- Each consumer affected is a separate violation.

The court must also consider the following when determining the civil penalty:

- Number of affected consumers;
- The severity of the violation;
- Sensitivity of the data in question;
- Size, nature, and complexity of the controller or processor's business;
- Any precautions are taken by the controller or processor to prevent the violation.

Similarly, appropriate relief may also be awarded to each affected consumer. In exceptional circumstances where the court determines a controller or processor intentionally violated a provision of TIPA, they may award treble damages.

However, a violation of TIPA cannot serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under TIPA or other law.

How an Organization Can Operationalize TIPA

Here are some practical steps an organization can take to operationalize compliance with TIPA within their daily operations:

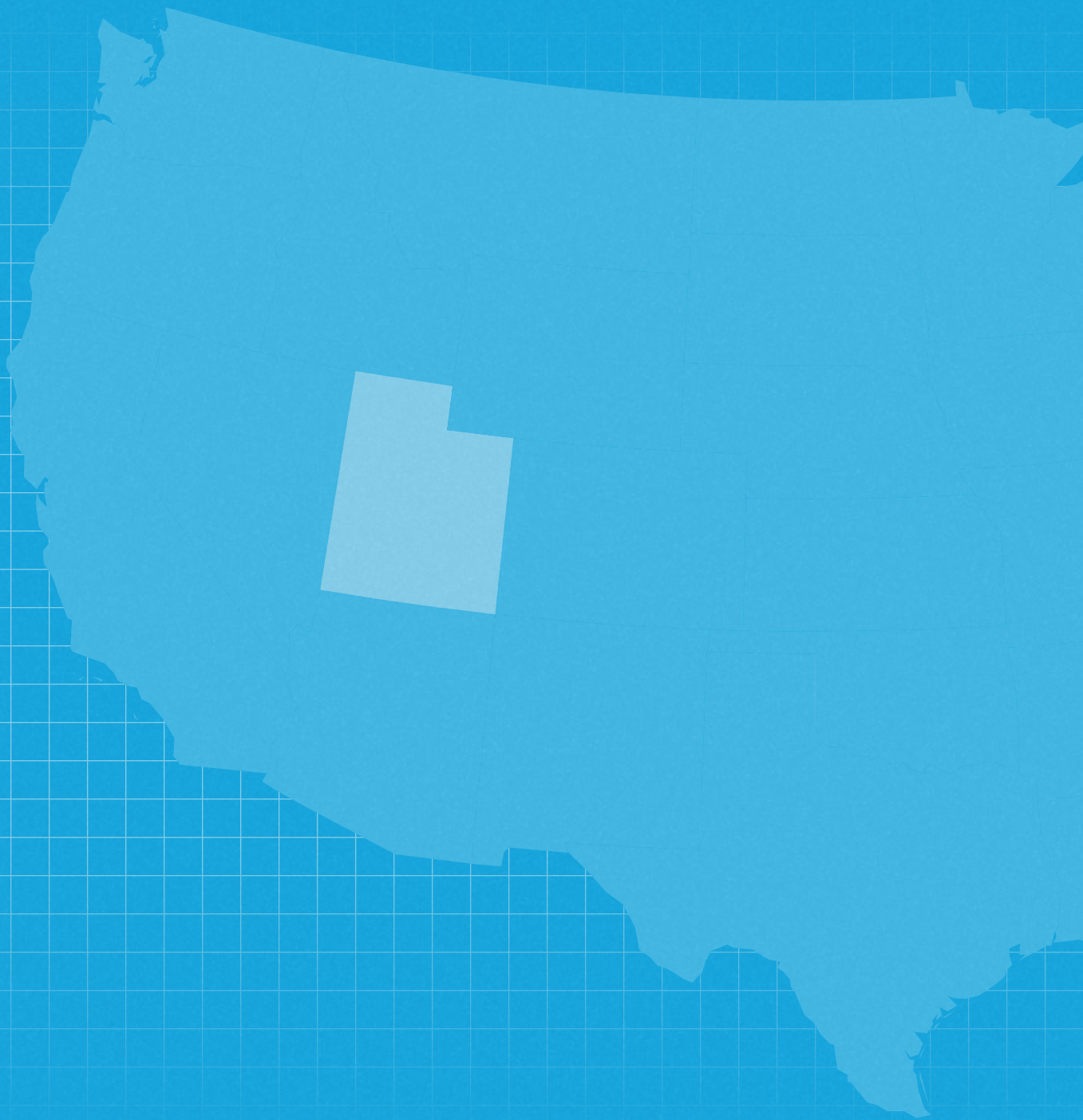
- Conduct and document regular data protection impact assessments while ensuring appropriate maintenance of records in case these assessments are requested by the Attorney General & Reporter;
- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the disclosed purposes;
- Implement, maintain, and monitor strict data security practices;
- Ensure all data processing activities are conducted per the disclosed purposes or purposes compatible with

disclosures unless expressly consented to by the consumer;

Have appropriate measures in place to collect and record consumer consent related to all major data processing activities, especially the sensitive data concerning a known child;

Adopt measures that allow for prompt responses to any consumer rights requests.

Utah's Consumer Privacy Act



What is UCPA?

On March 24, 2022, Utah Governor Spencer Cox signed the Utah Consumer Privacy Act (UCPA), making Utah the fourth US state to pass comprehensive privacy legislation after California, Virginia, and Colorado. The new privacy law empowers Utah citizens with greater personal data rights and safeguards.

The Utah Consumer Privacy Act will go into effect on December 31, 2023. In particular, the UCPA is substantially influenced by the Virginia Consumer Data Protection Act (VCDPA). The UCPA takes an easier, more business-friendly stance on consumer privacy than the Virginia Consumer Data Protection Act ("VCDPA"), the Colorado Privacy Act ("CPA"), and the California Privacy Rights Act ("CPRA").

Who Needs to Comply with the Law?

Material Scope

The UCPA applies to any organization that:

- Conducts business in the state of Utah or creates a product or service aimed toward Utah residents; and
- Has an annual revenue of \$25,000,000 or more; and
- Satisfies one or more of the following additional thresholds:
 - Controls or processes the personal data of 100,000 or more customers during a calendar year; or
 - Derives over 50% of the organization's gross revenue from the sale of personal data.

Notably, the UCPA also provides for certain exceptions; for example, the UCPA does not apply to: Notably, the UCPA also provides for certain exceptions; for example, the UCPA does not apply to:

- It's tribes and carriers;
- Institutions of higher education and nonprofits; and
- A governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity;
- Certain types of data used by credit and consumer reporting agencies;

Information of financial institutions or affiliates governed by the Gramm-Leach-Bliley Act;

Any personal information of consumers collected or used for consumer credit scoring and reporting is protected under the federal Fair Credit Report Act (FCRA);

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994;

Personal data regulated by the federal Family Educational Rights and Privacy Act (FERPA) and related regulations;

Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act;

Any health information, records, data, and documents protected and covered under HIPAA, and other federal or state medical laws, including patient information, identifiable private information for purposes of the Federal Policy for the protection of Human Subjects, patient safety work product, de-identified medical data, and medical data for public health use or medical research under HIPAA or any other medical law or policy, information maintained by a healthcare facility/provider, or information used only for public health activities and purposes;

Protection of Human Subjects, patient safety work product, de-identified medical data, and medical data for public health use or medical research under HIPAA or any other medical law or policy, information maintained by a healthcare facility/provider, or information used only for public health activities and purposes;

Personal data is maintained for employment records.

Territorial Scope

The UCPA applies only to for-profit businesses that conduct business in the state of Utah or sell products and services there. It only protects consumers who are residents of the state of Utah.

Obligations for Organizations Under UCPA

Under the UCPA, data controllers have multiple obligations, such as:

Non-Discrimination Requirements

Data controllers are prohibited from discriminating against consumers who exercise their rights by:

- denying a consumer a good or service;
- charging a varied price or rate to a consumer for a good or service; or
- offering a different level of quality of a product or service to the consumer.

The law, however, does not prevent a controller from offering a distinct rate (including discounts or product/service at zero fee), quality, or selection of a product or service to the consumer if: the consumer has opted out of targeted advertising; or

the offer relates to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Consent Requirements

The UCPA lays significant guidelines pertaining to processing the personal data of children. Data controllers processing the personal data of children under the age of 13 must get verified parental consent before processing their personal data. Additionally, personal data must be processed in compliance with the Children's Online Privacy Protection Act (COPPA).

The UCPA does not require opt-in consent to process a consumer's sensitive data. But rather, it lays down mandatory notice requirements, outlining that in case of processing sensitive data collected from a consumer, it should first present the consumer with a clear notice along with a method and opportunity to opt-out of processing of its sensitive data.

Moreover, in the case of the processing of personal data concerning a known child, the consumer should process the data in accordance with the federal Children's Online Privacy Protection Act and the act's implementing regulations and exemptions.

Privacy Notification/ Privacy Policy Requirements

Under the UCPA, consumers must be given a reasonably accessible, conspicuous, and unambiguous privacy notice by the controller. Privacy notices must include the following information:

- The types of personal data that the controller processes;
- The purpose for data processing;
- How consumers can exercise their opt-out rights if personal data is transferred to a third party or used for targeted advertising of personal data that the data controller shares with third parties (if any);
- The types of third parties with whom the controller may share personal data (if any).

Security Requirements

Data controllers must establish, implement, and maintain acceptable administrative, technological, and physical data security practices to preserve the confidentiality and integrity of personal data and reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data. A controller should use data security practices that align with its business size, scope, and type and are appropriate for the volume and nature of the personal data it deals with.

Non-Waiver of Consumer Rights

Under UCPA, it is also stated that any provision of a contract that purports to waive or limit a consumer's right is void.

Processing De-Identified Data or Pseudonymous Data

UCPA does not require a controller or processor to reidentify de-identified data or pseudonymous data, or obtain, maintain, or access data in identifiable form for the purpose of allowing the controller or processor to associate a consumer request with personal data. The controller is also not required to comply with an authenticated consumer request to exercise a right under the law, if:

- Either the controller does not have the reasonable capacity to associate the request with the personal data, or it would be unreasonably burdensome for it to associate the request with the personal data;
- personal data is not being used by the controller to recognize or respond to the consumer who is the subject of the personal data; and

personal data is not being sold or disclosed to any third party other than a processor.

Moreover, data subject rights do not apply to pseudonymous data.

Processor/Service Provider Agreements

The UCPA requires data controllers to engage in contracts with data processors that govern the nature, purpose, and duration of the processing of personal data, the type of data subject to processing, and the rights and obligations of parties. Also, these contracts should also bind the processor to a duty of confidentiality pertaining to the processing of personal data.

Moreover, any subcontractor pursuant to a written contract engaged by a processor is also bound by the same obligations. Processors must follow the controller's instructions and assist the controller in fulfilling his or her obligations, including those relating to the security of personal data processing and security breach notifications.

Data Subject Rights Fulfillment

Under the UCPA, consumers have the following rights:



Right to Access

Consumers have the right to confirm whether a controller is processing their personal information and access it.



Right to Delete

Consumers have the right to request the deletion of the personal data they have provided to the controller. However, the UCPA does not give consumers the right to have all their personal data held by a controller deleted - only personal data provided to the controller by the consumers themselves can be requested to be deleted.



Right to Data Portability

Consumers have the right to obtain a copy of their personal data previously given to the controller. The data should be portable and readily usable to the extent that is technically feasible and practical. Moreover, the copy should allow the consumer to send data without hindrance to another controller, where the processing is done automatically.



Right to Opt-out of Processing

Consumers have the right to opt-out of the processing of their personal data to evade targeted advertising. Consumers can also opt-out of the sale of their personal data. Finally, as previously mentioned, consumers can opt-out of the collection of their sensitive personal data.

Means to submit DSR request

A consumer may exercise a right by submitting an authenticated request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise. In the instance of processing personal data concerning a child, the parent or legal guardian of the child can exercise a right on the child's behalf. In the case of processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangements under Title 75, Chapter 5, Protection of Persons Under Disability and Their Property, the guardian or the conservator of the consumer shall exercise a right to the consumer's behalf.

Time period to fulfill DSR request

A controller shall comply with a consumer's request to exercise a right within 45 days after the day on which a controller has received that particular request. The controller then shall take action on the consumer's request and inform the consumer of any action taken on the consumer's request.

Extension in the time period

An additional 45 days can be granted if it is reasonably necessary to comply with the request, keeping in mind the complexity of the request or the volume of the requests received by the controller. In such cases, the controller is to inform the consumer of the extension and provide reasons for the extension.

Charges

Controllers are not allowed to charge a fee for responding to a request under the law apart from certain situations. If the request is a consumer's second or subsequent request within the same 12-month period, a controller may charge a reasonable fee. A controller may also charge a reasonable fee to cover the administrative costs of complying with a request or refuse to act on a request if:

the request is excessive, repetitive, technically infeasible as per the law; or

the controller considers that the primary goal for the submitted request was something other than exercising a right; or

the request disrupts or imposes an undue burden on the resources of the controller's business.

Appeal against refusal

The data controller may choose not to take action on a consumer's DSR request. It must provide the consumer with the reasons for which it did not take action within the 45 days time period of receiving the DSR request. The data controller may also choose not to honor the request if it cannot authenticate it using commercially reasonable efforts. It is also significant to note that there exists no right of appeal for the consumer in case the controller denies the consumer's requests under UCPA however, the burden of proof to prove the reason for refusal of the consumer's request will lie with the data controller.

Regulatory Authority

Utah's Attorney General has exclusive enforcement authority of Utah's Consumer Privacy Act. However, the enforcement method employs a new multi-layered strategy. The UCPA tasks Utah's Consumer Protection Division to manage a system to accept consumer complaints and investigate whether a claimed infringement is valid.

If the Director of the Division has reasonable cause to think that extensive evidence (of a violation) exists, they must refer the case to the state Attorney General. Once a referral from the division is received, the Attorney General may initiate proceedings against a controller or processor for a violation.

Limitations

The obligations imposed under TIPA do not restrict a controller's or a processor's ability to:

Data processed for legal obligations

This law does not prevent a controller or processor from complying with other applicable laws, asserting or defending legal claims, or cooperating with government authorities or investigations.

Data processed to perform contractual obligations

Nothing in this law restricts a controller or processor from complying with contractual obligations with the consumer.

Data processed to protect life and physical safety

Nothing in this legislation prevents a controller or processor from taking prompt action to defend an interest that is vital to the consumer's or another natural person's life or physical safety, and if the processing cannot be justified by another legal basis.

Data processed for security purposes

Nothing in this law prevents a controller or processor from processing data to prevent, detect, protect

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

Data processed for internal purposes

Nothing in this law restricts a controller or processor from processing personal data to conduct internal research to identify, improve or repair products, services, or technology, including technical errors that impair existing or intended functionality, or undertake internal operations reasonably aligned with the consumer's expectations for the performance of a service or provision of a product.

Penalties for Non-Compliance

The UCPA empowers the Attorney General's Office to pursue enforcement action and impose penalties. All alleged violations of the UCPA have a 30-day cure period, during which the Attorney General will provide the controller or processor a written notice identifying each alleged violation and an explanation of the basis for each allegation.

Following this, the controller or processor can provide the attorney general an express written statement detailing that the violation has been cured and that no further violation of the cured violation will occur, thereby curing the violation.

In the event of a controller failing to cure the violation or, after curing a noticed violation, continues to violate the sections under the law, the UCPA also allows the attorney general to recover actual damages to the consumer on their behalf (there is no private right of action within the law) and a civil penalty of up to \$7,500 for each violation.

How an Organization Can Operationalize the UCPA

To comply with UCPA, organizations must:

Determine whether they meet the jurisdictional threshold of UCPA, including whether they hold personal data of Utah residents and whether they meet the data volume threshold;

Determine their data inventories and classify data stores containing personal data of Utah residents;

Using official policies and privacy notices, make it clear how personal data is processed;

Develop formal policies and procedures for data collection (specifically for sensitive data) processing;

Establish a robust framework for data subject requests;

Develop a robust consent framework that swiftly processes consent obligations;

Allow Utah residents to exercise their opt-out rights in cases where the organization sells their personal data or uses it for targeted advertising;

Have technical and organizational security measures in place to protect their processing activities; and

Conduct a rigorous analysis of their data handling capabilities and third-party processor agreements.

Virginia Consumer Data Protection Act



What is VCDPA?

Virginia became the second US state to pass a comprehensive consumer data protection law that can be considered to be at par with other major state data privacy laws i.e. the California Consumer Protection Act (CCPA) or the Consumer Privacy Rights Act (CPRA) and Washington Privacy Act (WPA). Virginia Consumer Data Protection Act (VCDPA) provides comprehensive privacy rights to state residents and imposes a new set of obligations and duties on businesses managing consumer personal data. VCDPA went into effect on January 1, 2023.

Who Needs to Comply with VCDPA?

Scope

VCDPA applies to all businesses in Virginia or those who produce products or services that are targeted to residents of Virginia and “control and process” the personal data of:

at least 100,000 Virginia residents; or

for an entity that derives over half (50%) of its gross revenue from the sale of personal data of at least 25,000 Virginia residents.

Exemptions

The following entities are exempt from complying with the VCDPA:

Public/government bodies

Any body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth;

GLBA entities

Financial Institutions or data that is subject to Title V of the federal Gramm-Leach-Bliley Act (GLBA);

HIPAA/HITECH covered entities

Any covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services (HHS) pursuant to the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health Act (HITECH);

COPPA-compliant entities

Controllers and processors that comply with the verifiable parental

consent requirements of the federal Children's Online Privacy Protection Act (COPPA) will be deemed to be in compliance with the obligation to obtain parental consent.

Obligations for Organizations Under VCDPA

Transparency

Controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice containing specific information, including categories of data it shares or sells (including for targeted advertising) and means for consumers to exercise their rights.

Accountability

Controllers must undertake Data Protection Assessments (DPAs) before conducting certain types of risky processing, protect de-identified data from reidentification, comply with data subject requests made by consumers, and ensure data processors it contracts with comply with the duties prescribed under this law.

Purpose Limitation And Data Minimization

Controllers must not collect consumers' unnecessary personal data or process it for purposes beyond what was disclosed to consumers without gaining their consent.

Non Discrimination

Controllers must not process personal data to discriminate against the consumer in any way - including discrimination for exercising their data privacy rights.

Consent Management

Controllers must not process sensitive personal data (including data of minors) unless it has the consumer's express consent (or parents/guardians of a minor child).

Data Security

Either the controller does not have the reasonable capacity to associate the request with the personal data, or it would be unreasonably burdensome for it to associate the request with the personal data;

personal data is not being used by the controller to recognize or respond to the consumer who is the subject of the personal data; and

personal data is not being sold or disclosed to any third party other than a processor.

Moreover, data subject rights do not apply to pseudonymous data.

Processor/Service Provider Agreements

The UCPA requires data controllers to engage in contracts with data processors that govern the nature, purpose, and duration of the processing of personal data, the type of data subject to processing, and the rights and obligations of parties. Also, these contracts should also bind the processor to a duty of confidentiality pertaining to the processing of personal data.

Moreover, any subcontractor pursuant to a written contract engaged by a processor is also bound by the same obligations. Processors must follow the controller's instructions and assist the controller in fulfilling his or her obligations, including those relating to the security of personal data processing and security breach notifications.

Data Subject Rights

All consumers may invoke the following rights by sending a verified request to the data controller (in the case of a child, the parent/guardian may send the request on behalf of the child):



Confirm

The consumer has a right to confirm whether or not a controller is processing his/her personal data.



Access

The consumer has a right to access the personal data collected and processed about him/her by the data controller.



Rectify

The consumer has a right to have inaccurate personal data being stored or processed by the data controller be corrected.



Delete

The consumer has the right to have his/her personal data stored or processed by the data controller deleted.



Port

The consumer has a right to obtain a copy of his/her personal data in a portable, technically feasible, and readily usable format that allows the consumer, where the processing is carried out by automated means, to transmit the data to another controller without hindrance.



Opt-Out

The consumer has the right to opt-out of the processing of 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.

Time period to fulfill DSR request

All data subject rights requests (DSR requests) must be fulfilled by the business within a 45-day period.

Extension in the time period

Businesses may seek an extension of 45 days in fulfilling the request depending on the complexity and number of the consumer's requests.

Denial of DSR request

If a DSR request is to be denied, the business must inform the consumer of the reasons within a 45 days period. Businesses can deny DSR requests from a consumer if they are unfounded, excessive, or repetitive.

Appeal against refusal

Consumers have a right to appeal the decision for refusal of the grant of the DSR request. The appeal must be decided within 60 days.

Limitation of DSR requests per year

Information provided in response to a consumer request shall be provided by a controller up to twice annually per consumer.

Charges

DSR requests must be fulfilled free of charge. However, if requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request.

Regulatory Authority

The Virginia Attorney General has the exclusive authority to enforce the VCDPA by bringing an action in the name of the Commonwealth or on behalf of persons residing in the Commonwealth as well as reasonable expenses incurred in investigating and preparing the case, including attorney fees against violators.

Any Important Exemptions

The VCDPA does not apply to:

Data processed in an employment or commercial (business-to-business) context

Personal data processed by a controller, processor, or third party for the following reasons are exempt from the application of this law:

- o in the course of an individual applying to, employed by, or acting as an agent of a controller, processor, or third party as long as the data is processed within that context;
- o necessary for the controller, processor, or third party to retain to administer benefits for another individual related to the individual highlighted in part (a) i.e. an employee or contractor, as long as the data is used for the purposes of administering those benefits;
- o As the emergency contact information of an individual used for emergency contact purposes.

Data processed for household purposes or free speech: Nothing in this law should be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

Data processed for internal purposes

Nothing in this law restricts a controller or processor from processing personal data to conduct internal research to improve or repair products, services, or technology or to identify and repair technical errors that impair existing or intended functionality or to undertake internal operations reasonably aligned with the consumer's expectations for performance of a service or provision of a product.

Data processed for legal obligations

Nothing in this law restricts a controller or processor from complying with other applicable laws to claim or defend legal claims or cooperate with government authorities or investigations.

Data processed to protect life and physical safety

Nothing in this law restricts a controller or processor from taking immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person and where the

processing cannot be manifestly based on another legal basis.

Data processed for security purposes

Nothing in this law restricts a controller or processor from processing 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; or investigate, report, or prosecute those responsible for any such action.

Data processed for scientific purposes

Nothing in this law restricts controllers from engaging in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine:

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

Penalties for Non-Compliance

The Virginia Attorney General may issue a civil investigative demand to any controller or processor believed to be engaged in, or about to engage in, any violation.

Thus covered businesses must comply with the law or face civil penalties for non-compliance up to \$7500 for each violation as well as an injunction to stop the violation from continuing further.

How Organizations Can Operationalize VCDPA

Here are some steps a covered entity may take to ensure they're on track for effective compliance with the VCDPA:

Have a privacy policy that is easily understandable and communicates the organization's obligations and consumers' rights effectively;

Ensure all the company's employees and staff are acutely aware of their responsibilities under the law;

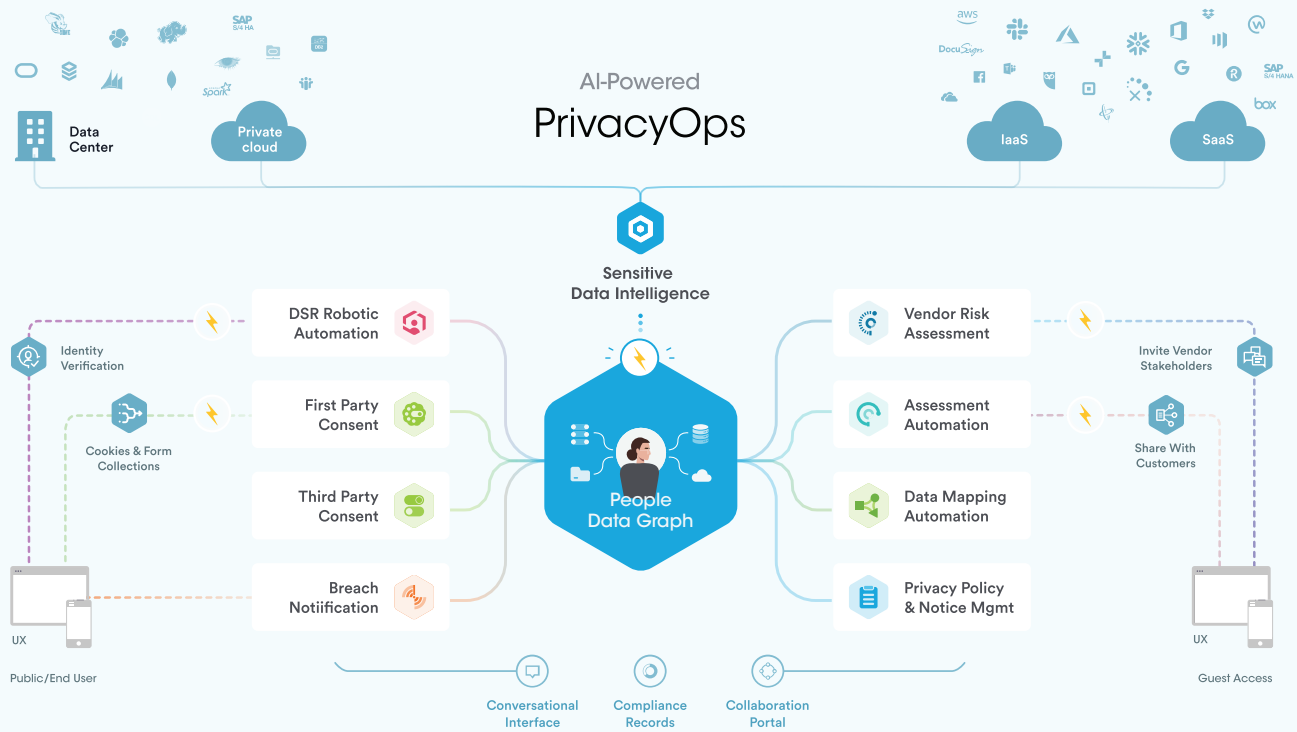
Have a compliant consent mechanism in place to capture express consent;

Communicate to all consumers what data is being collected on them;

Maintain proper channels of communication, allowing the consumers to exercise their data subject rights both freely and easily;

Have an appropriate system in place to record, review, and maintain all valid authorizations from consumers.

Meet Global Data Compliance with Securiti PrivacyOps



Securiti uses the PrivacyOps architecture to provide end-to-end business automation, combining reliability, intelligence, and simplicity. Securiti can assist you in complying with global privacy and security standards cost-effectively.

[Request Demo](#)