

DENTONS

National Apartment Association

Guidance on U.S. State Comprehensive Consumer Privacy Law.

NAA LEGAL AFFAIRS

National Apartment Association (NAA) Legal Disclaimer

The information supplied in this resource and the opinions expressed are exclusively those of the author(s). There is no intention to give, and nothing here should be taken as, legal advice by the National Apartment Association (NAA). The information provided is general in nature and is not intended to address a particular legal issue. The purpose of this information is to educate and to provide food for thought.

Copies of this presentation may not be distributed to others without the express written permission of the authors or the National Apartment Association. The information presented here is only valid at the time that the document is distributed.

Authors



Kyle W. Miller
Partner, Louisville
D +1 502 587 3517
kyle.miller@dentons.com



Dalton Cline
Associate, Louisville
D +1 502 587 3647
dalton.cline@dentons.com

Executive Summary

Twenty-three states have enacted comprehensive consumer privacy laws governing the processing of personal data. These laws impose significant compliance obligations on data Controllers, which include apartment building owners and property management companies that collect applications, lease records, payments, and maintenance requests.

This guidance document addresses six core compliance responsibilities for Controllers under these laws:

- **Privacy Program Governance**. Organizations must establish reasonable administrative, technical, and physical data security practices. These practices may vary depending on your jurisdiction. For example, Minnesota requires documented internal policies and a named privacy officer. California mandates formal employee training programs. Apartment owners should designate a privacy coordinator, develop written policies for resident data handling, and implement layered security measures.

- **Processing Conditions and Prohibitions**. Controllers must adhere to principles of data minimization, purpose specification, non-discrimination, and non-retaliation. Sensitive data categories, including biometric identifiers, precise geolocation, and data concerning minors, require heightened protection, often affirmative opt-in consent.

- **Risk Assessment**. Privacy Impact Assessments are required before engaging in Targeted Advertising, selling personal data, processing sensitive personal data, or using automated decision-making technology for Significant Decisions such as housing. Apartment owners using automated resident-screening tools should assess whether those tools meet the threshold for Automated Decision-Making Technology and document how human review is incorporated into rental decisions.

- **Public Disclosures**. Controllers must publish privacy notices describing data collection practices, purposes, and Third-Party disclosures. For example, California requires “just in time” notices at the point of collection and specific disclosures when using automated decision-making technology. Delaware requires adverse action notices when denying applications based on Third-Party data. Apartment owners should develop appropriate comprehensive privacy notices.

- **Contractual Requirements**. Data processing agreements with vendors must include specific provisions governing processing scope, confidentiality, data deletion, compliance demonstration, and audit rights. Apartment owners should review all vendor contracts—particularly with resident screening services, property management software providers, and payment processors—to ensure statutory compliance.

- **Data Subject Rights**. These laws grant individuals up to **13** rights, including rights to access, correct, delete, and port their personal data, as well as rights to opt-out of sales and Targeted Advertising. Controllers must establish intake mechanisms, verify requestor identity, confirm receipt, and effectuate or deny the request and inform the Data Subject within a certain time period (generally within 45 days with possible extensions), and provide appeal processes. Apartment owners should train leasing staff to recognize and promptly route resident privacy requests.

For apartment building owners operating across multiple states, the recommended approach is to adopt a compliance baseline aligned with the most restrictive requirements while monitoring jurisdiction-specific obligations such as Delaware's enhanced Third-Party due diligence requirements and Minnesota's mandatory written policy documentation. This document provides detailed guidance on each compliance obligation, including practical implementation steps tailored specifically to the apartment industry.

Contents

Executive Summary *3*
Introduction *6*
Key Concepts *9*
Privacy Program Governance *15*
Core Program Components 15
Jurisdiction-Specific Enhanced Requirements 15
Processing Conditions and Prohibitions *18*
Risk Assessment *19*
Privacy Impact Assessment 19
Public Disclosures *22*
Privacy Notice 22
Notice at Collection 22
Adverse Action Notice 23
Automated Decision-Making Technology Notice 23
Contractual Requirements *25*
Processors 25
Third-Parties 26
Data Subject Right Requests *28*
Available Data Subject Rights 28
Intake of Data Subject Right Requests 33
Evaluating Data Subject Right Requests 34
Responding to Data Subject Right Requests 35
Appeals 38
Glossary *39*
Appendix: Comprehensive Consumer Privacy Law Statutes *40*

Introduction

Since the passage of the California Consumer Privacy Act in 2018, 22 other states[1] have passed consumer privacy laws and regulations governing the processing of "personal data."[2]

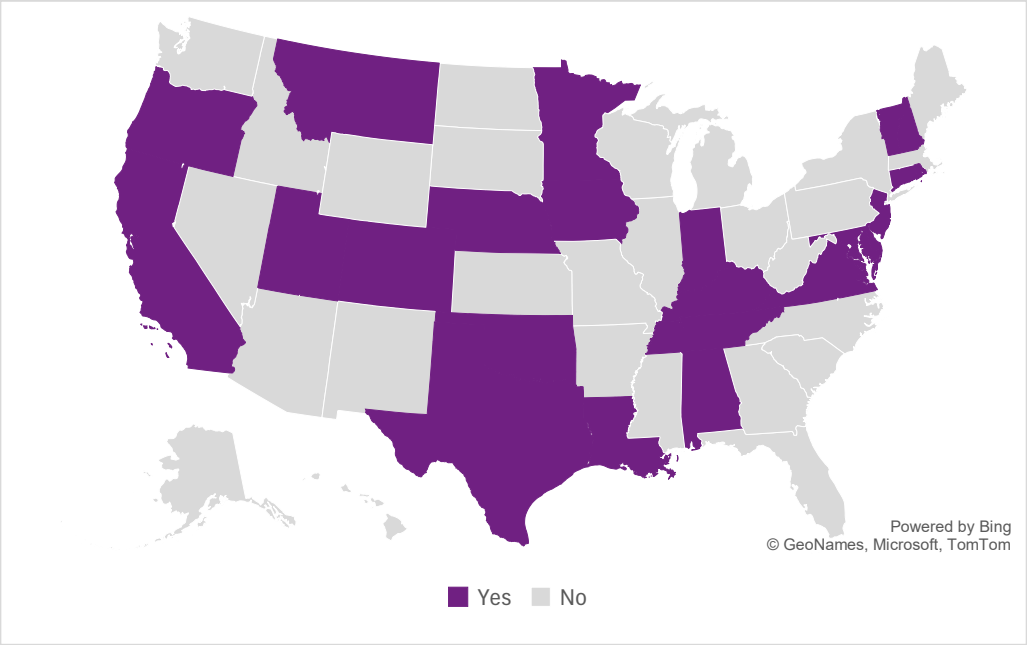

Figure 1: States with Comprehensive Consumer Privacy Laws

As of October 2026, nearly half of the country will be protected by a Comprehensive Consumer Privacy Law. By January 1, 2028, the laws of four additional states (Alabama, Louisiana, Oklahoma, and Vermont) will have become effective.

[1] See Appendix: Comprehensive Consumer Privacy Law Statutes for a complete list of statutory citations, where available.
[2] Terms of art are bold and italicized on first use. See the Glossary below for definitions.

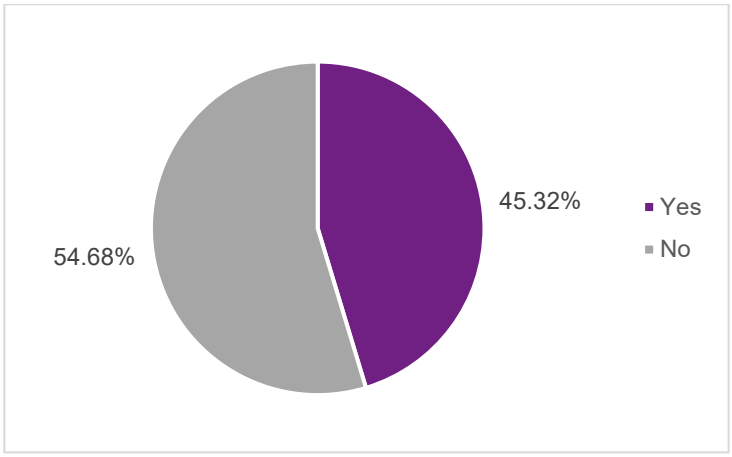

Figure 2: % of Population Protected by US State Comprehensive Consumer Privacy Law effective October 2026[3]

But, as the proliferation of these laws across the country shows no sign of slowing down, that percentage is sure to change.

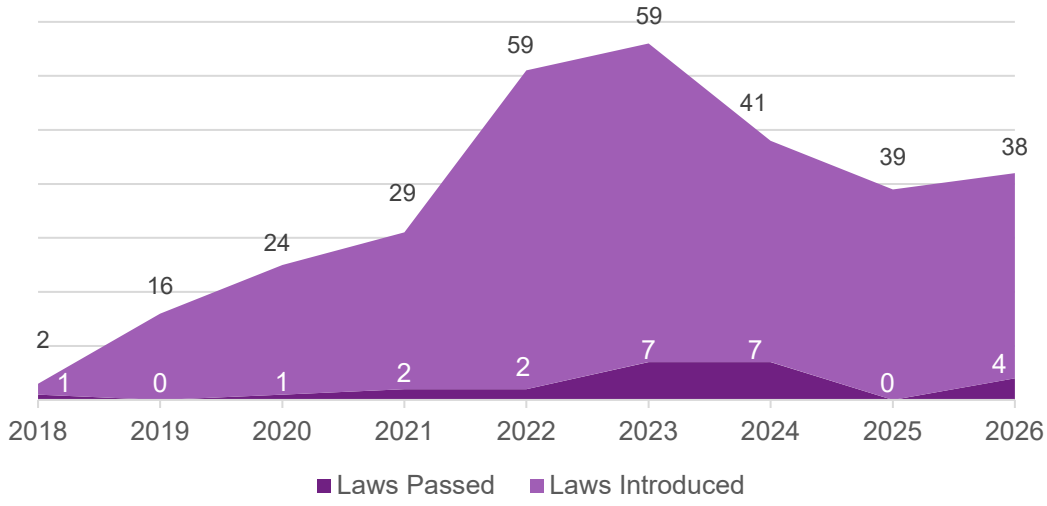

Figure 3: Growth of US State Comprehensive Consumer Privacy Laws

A "***Controller***" has six core compliance responsibilities under US State Comprehensive Consumer Privacy Law:

1. Establish a privacy governance program with policies and procedures overseen by an officer
2. Abide by certain conditions and prohibitions when "***processing***" personal data

[3] Based on US Census Population Estimate as of July 1, 2025.

3. Conduct risk assessments with specific elements of analysis prior to particular personal data processing activities
4. Provide public disclosures containing statutorily required information
5. Execute compliant contracts with "***Processors***" and "***Third Parties***" containing statutorily required terms
6. Effectuate "***Data Subject***" Right Requests

This guidance document provides a brief overview of compliance obligations with each of these responsibilities.

Key Concepts

Jurisdictional Thresholds

Each of the U.S. State Comprehensive Consumer Privacy Laws have a unique jurisdictional threshold based on an entity's jurisdiction, revenue, volume of personal data processing and revenue from the sale of personal data. Determining applicability is a multi-step process: First, the entity must "do business" in the state or produce products or services "targeted" to residents of that state. Then, the entity must surpass a particular revenue, personal data processing volume, or revenue from the sale of personal data threshold. Figure 4 below provides an overview of these thresholds.

Jurisdiction	Data Subject Volume	Sales % Revenue + Volume
NE & TX[4]	Any	Any % + Any
CT	≥ 35,000	Any % + Any
VT	≥ 35,000	Any % + 3,000
CA	≥ 100,000	> 50% + Any
DE, MD, & RI	≥ 35,000	> 20% + ≥ 10,000
NH	≥ 35,000	> 25% + ≥ 10,000
MT	≥ 25,000	> 25% + ≥ 15,000
AL	≥ 25,000	> 25% + Any

[4] Nebraska and Texas are unique in that, rather than using volume and revenue thresholds, their statutes apply to any for-profit entity that is not a "small business" as defined by the US Small Business Administration ("SBA"). The SBA states that "size standards vary by industry and are generally based on the number of employees or the amount of annual receipts the business has." A business qualifies as a small business concern only by reference to a North American Industry Classification System ("NAICS") code(s). Most size standards are stated in terms of either receipts or employees. To help business owners determine whether their businesses are small, SBA publishes a Table of Small Business Size Standards which lists the size standard that applies to each NAICS code. SBA has released a size standards tool to help businesses determine whether they qualify as small for purposes of Federal contracting.

LA	≥ 75,000	> 50% + Any
CO & NJ	≥ 100,000	Any % + ≥ 25,000
MT & OR	≥ 100,000	> 25% + ≥ 25,000
IN, IA, KY, OK, UT, & VA	≥ 100,000	> 50% + ≥ 25,000
TN	≥ 175,000	> 50% + ≥ 25,000

Figure 4: US State Comprehensive Consumer Privacy Law Volume and Revenue Comparison

Several jurisdictions have additional bases for applicability. For example, the Connecticut Data Privacy Act applies to any entity that processes "sensitive" personal data, and the Louisiana Data Privacy Act and California Consumer Privacy Act would apply to a business that generated more than $27million in the prior 12 months. To receive a free report summarizing which jurisdictional thresholds you may pass, consult Dentons complimentary U.S. Comprehensive Consumer Privacy Law Threshold Assessment or scan the QR code at the end of this report.

Personal Data

"Personal data" under U.S. State Comprehensive Consumer Privacy Law is any information that is linked or reasonably linkable to an identified or identifiable natural person. This definition is far broader than is often understood. While other laws such as those that govern data breaches cover specifically enumerated pieces of information that could be used for identity theft, like social security or driver's license numbers, under the Comprehensive Consumer Privacy Laws, *any* information that *is* linked or *could be* linked to a person is "personal data."

"***Anonymized data***" is information that was previously personal data that has been modified using irreversible statistical techniques or methods so that the information can no longer reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable Data Subject or a device linked to such individual.

Processing

U.S. State Comprehensive Consumer Privacy Law imposes obligations on entities that "process" personal data. "Processing" personal data is any operation or set of operations performed on

information, whether or not by automatic means. “Processing” covers all parts of the data lifecycle.[5]

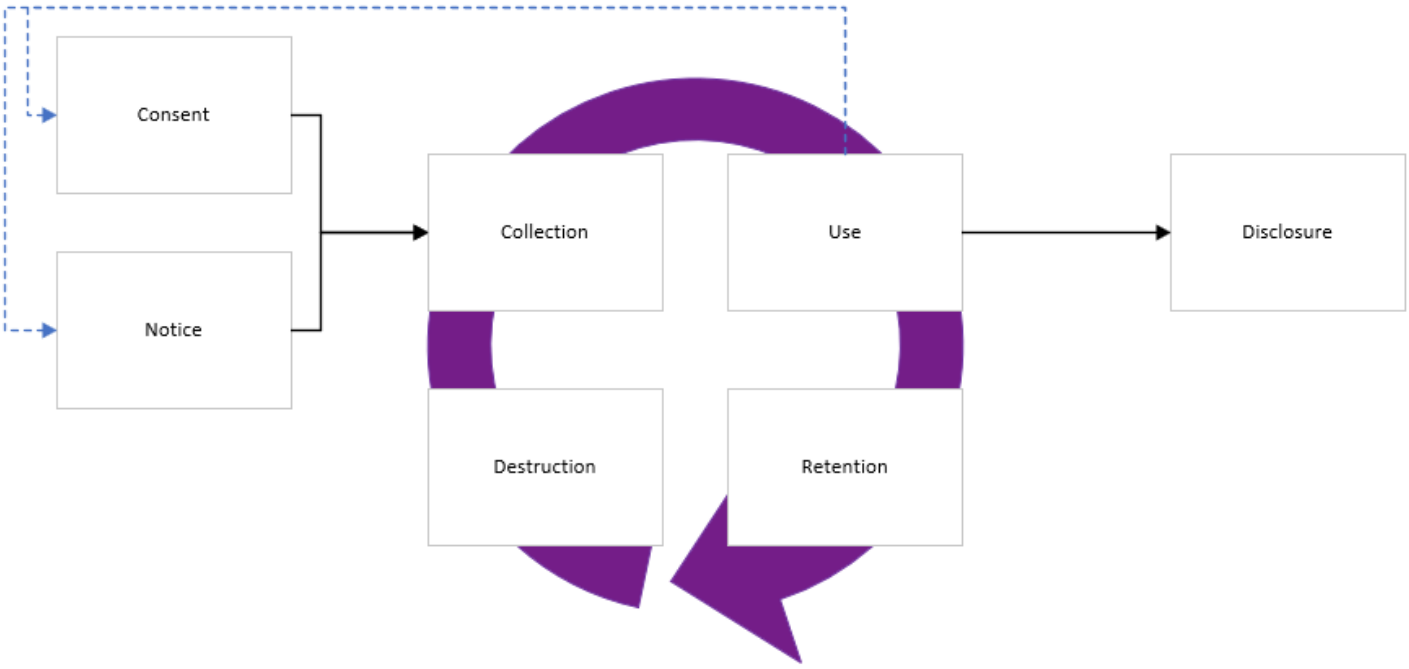

Figure 5: Data Lifecycle

Data Subjects

A “***Data Subject***” is the identified or identifiable natural person to whom the personal data relates. The majority of U.S. State Comprehensive Consumer Privacy Laws only apply to the personal data of “consumers” (that is, individuals acting in their personal, individual, or household capacities) including renters. However, the laws of California, and in some cases Connecticut and Delaware, also apply to individuals in their commercial, employment or professional capacities.

Roles

When an entity processes personal data, the entity’s responsibilities under U.S. State Comprehensive Consumer Privacy Law depend on the entity’s role as either a Controller, a Processor, or a Third Party.

- Controller: A person who, alone or jointly with others, determines the purpose and means of processing personal data.
- Processor: A person who processes personal data on behalf of a Controller.
- Third Party: A person other than the Data Subject, the Controller, a Processor, or an affiliate of the Controller or Processor.

[5] Diagram adapted from “An Introduction to Privacy for Technology Professionals,” ed. Travis Breaux (2020), pg. 12.

"Sale" of Personal Data

There is a jurisdictional split in the U.S. regarding the definition of "sale." The majority of jurisdictions define "sale" as the exchange of personal data for monetary **or other valuable consideration** by the Controller to a Third Party. A minority of jurisdictions limit the definition of "sale" to the exchange of personal data for **only** monetary consideration to a Third Party.

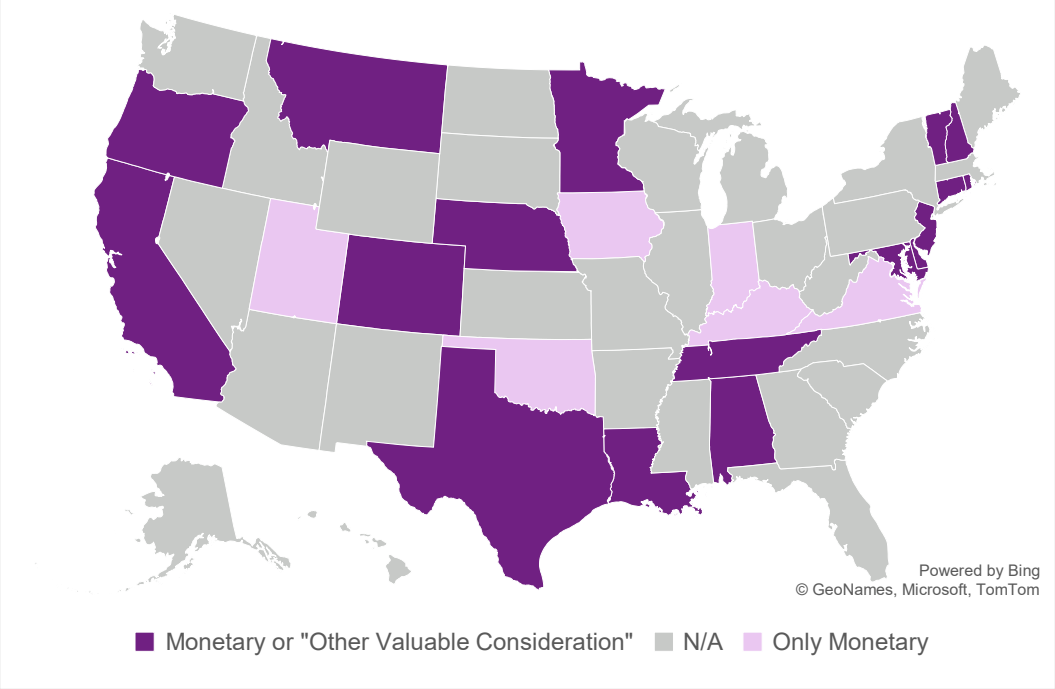

Figure 6: Definition of "Sale as of October 2026"

Although what constitutes "the exchange of personal data… to a Third Party… for… valuable consideration" has not been interpreted by enforcement action or sub-regulatory guidance in most jurisdictions, the California Attorney General has interpreted a similar provision in the California Consumer Privacy Act (**CCPA**) to mean that *any* disclosure of personal data to a Third-Party may be a "sale."[6] For example, in *California v. Sephora USA, Inc.*, the California Attorney General stated that Sephora had received "valuable consideration" in the form of website analytics when they disclosed personal data collected through online tracking technologies to a Third-Party, and that this disclosure therefore constituted a "sale" under the CCPA.

Data and Entity Exemptions

Each of the U.S. State Comprehensive Consumer Privacy Laws recognizes that certain organizations and certain categories of data are already subject to robust regulatory frameworks

[6] *See*, Complaint, California v. Sephora USA, Inc., No. CGC-22-601380 (S.F. Super. Ct. Aug. 23, 2022) ("if companies make consumer personal information available to third parties and receive a benefit from the arrangement—such as in the form of ads targeting specific consumers—they are deemed to be "selling" consumer personal information under the law,"), Complaint, California v. DoorDash, Inc., No. CGC-24-612520 (S.F. Super. Ct. Feb. 21, 2024) ("The disclosure of "the personal information of [DoorDash's] California customers to a marketing co-op in exchange for the opportunity to send mailed advertisements to customers of the other participating businesses… is a sale of personal information under the CCPA").

at the federal level. To avoid duplicative or conflicting compliance obligations, the laws carve out two principal categories of exemptions: Entity-level exemptions (which excuse entire organizations from the law's requirements) and data-level exemptions (which exclude specific types of information regardless of who holds them).

Entity-level exemptions remove entire categories of organizations from a state privacy law's reach. The most common entity-level exemptions across the states include:

- **HIPAA-covered entities and business associates**. Health care providers, health plans, and clearing houses subject to the federal Health Insurance Portability and Accountability Act (HIPAA) are exempt in virtually every state. In practical terms, this means a hospital or health insurer already complying with HIPAA's privacy, security, and breach notification rules does not separately need to comply with the state privacy law.

- **Financial institutions subject to the Gramm-Leach-Bliley Act (GLBA)**. Banks, credit unions, insurance companies, and their affiliates that are governed by Title V of the GLBA—which already imposes data-sharing disclosure requirements—are similarly excluded. This means a consumer's bank, for example, falls outside the state privacy law's scope.

- **Nonprofit organizations**. Most states exempt nonprofits entirely. Virginia, for example, exempts any corporation organized under its Nonstock Corporation Act, and Indiana exempts any nonprofit organization outright. However, some states, such as Oregon and Maryland, take a narrower approach, exempting only nonprofits engaged in specific activities such as insurance fraud detection or assisting first responders, rather than granting a blanket exemption.

- **Government agencies and institutions of higher education**. State and local governmental bodies are universally excluded, as are colleges and universities in most states.

Data-level exemptions apply to specific categories of information, regardless of who holds the data. Key categories include:

- **Protected health information (PHI) under HIPAA.** Even when an entity is not itself a HIPAA-covered entity, if it processes data that qualifies as PHI under HIPAA, that particular information is exempt from state privacy laws.

- **Employee and business-to-business (B2B) data.** Many states exclude personal data collected in the employment context, such as job applications, payroll records, and benefits administration, as well as emergency contact information. In plain terms, this means the privacy rights in these laws generally do not cover the data your employer collects about you in your capacity as an employee. Notably, California's CCPA is one of the few states that regulates employee and B2B data.

- **Publicly available information.** Data lawfully made available through government records or widely distributed media is excluded from the definition of personal data in most states. For Data Subjects, this means information already in the public record, such as property filings or professional licenses, generally cannot be the basis for a privacy rights request.

- **Data governed by other federal laws.** Information regulated under the Fair Credit Reporting Act (**FCRA**), the Family Educational Rights and Privacy Act (**FERPA**), and the Driver's Privacy Protection Act ("**DPPA**") is exempt in most states, reflecting a legislative judgment that these existing federal frameworks provide sufficient protection.

Significant Decision

A "***Significant Decision***" is a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, or independent contracting opportunities or compensation, or health-care services.

Automated Decision-Making Technology

Automated Decision-Making Technology (***ADMT***) is defined in California as "any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking" (emphasis added).[7]

The California Privacy Regulations define "substantially replace human decisionmaking" as using "the technology's output to make a decision without human involvement." Whether there was "human involvement" in turn turns on a three-part test:[8]

- **Competence**: The human reviewer must know how to interpret and use the technology's output to make the decision.
- **Independent Review**: The human reviewer must review and analyze the output of the technology, and any other information that is relevant to making or changing the decision.
- **Authority**: The human reviewer must have the authority to make or change the decision based on their analysis.

[7] Cal. Code Regs. tit. 11, § 7001(e)
[8] Cal. Code Regs. tit. 11, § 7001(e)(1).

Privacy Program Governance

Core Program Components

Every jurisdiction requires certain Public Disclosures, and almost every jurisdiction requires a Risk Assessment prior to certain processing activities that present a heightened risk of harm, which are discussed below. An additional universal requirement is to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect personal data.

The standard of reasonableness varies slightly across jurisdictions. New Jersey specifies that practices must secure personal data "during both storage and use from unauthorized acquisition."[9] Colorado's regulations further enumerate factors for determining "reasonable and appropriate" safeguards, including applicable industry standards and frameworks, organizational size and complexity, data sensitivity, and the risk of harm to Data Subjects.[10] Rhode Island and Utah require practices to "reduce reasonably foreseeable risks of harm to customers relating to the processing of personal data."[11]

Jurisdiction-Specific Enhanced Requirements

Mandatory Written Internal Policies and Procedures

Minnesota is unique for requiring Controllers to "document and maintain a description of policies and procedures" that addresses a range of governance topics, including the name and contact information for the Controller's chief privacy officer (or equivalent), policies for Privacy by Design, Data Subject rights, security controls, data minimization, purpose limitation, and violation remediation.[12] The requirement to have a named privacy officer role is highly jurisdiction-specific; no other state in the consolidated standard mandates a named privacy officer role. And while the policy requirements are unique, Minnesota's statute is nuanced: It requires the Controller to document a *description* of these policies "where applicable," meaning the statute mandates the documentation exercise but does not necessarily require that each listed policy exist—only that any that do exist are included in the description.

Formal Employee Privacy and Security Training Programs

California imposes the most prescriptive training requirements. Controllers must inform individuals responsible for handling Data Subject inquiries about the Controller's information practices or

---

[9] N.J. Stat. § 56:8-166.12(a)(3).
[10] 4 Colo. Code Regs. § 904-3:6.09.
[11] 6 R.I. Gen. Laws § 6-48.1-7(s), Utah Code § 13-61-302(2)(a)(ii).
[12] Minn. Stat. § 325M.18(a)(2).

CCPA compliance of all requirements in the CCPA.[13] California also requires that employees whose duties include participation in processing subject to a risk assessment be included in the assessment.[14]

Data Retention and Deletion Schedules

Several jurisdictions impose specific retention and deletion requirements:

- **Montana** requires retention of privacy impact assessment related to minors for the longer of three years after processing operations cease or the date the Controller ceases offering the online service, product, or feature.[15]
- **Colorado** requires retention of privacy impact assessments for at least 36 months,[16] while **California** requires at least 5 years after the processing activity ceases.[17]
- **California and Colorado** require retention of Data Subject Right Request records for at least 24 months.[18]
- **Colorado** requires retention of processing activities records demonstrating compliance with data minimization, purpose limitation, and children's data consent for as long as the processing activity continues and at least 24 months thereafter.[19]

Third-Party Due Diligence

Amendments to the Delaware Personal Data Privacy Act in 2026 added an explicit obligation on Controllers to assess the technical and organizational measures of any Third-Party (but not Processor) to whom the Controller discloses personal data. Delaware specifies that "reasonable due diligence involves, at a minimum, assessing the Third-Party through the use of questionnaires and review of relevant documents," with additional measures "commensurate with the sensitivity of the data disclosed."[20]

Practical Implementation Guidance

Designate a privacy coordinator, whether an internal employee or outsourced compliance professional, to oversee resident data handling. Develop a written privacy policy addressing how you collect, store, and secure resident applications, lease records, payment histories, and maintenance requests. Implement reasonable security measures such as encrypted digital storage, locked physical files, and access controls limiting staff access to personal data on a need-to-know basis. Train property managers and leasing agents on data handling practices,

---

[13] Cal. Code Regs. tit. 11, § 7100(a). Controllers that know or reasonably should know they process data of more than 10,000,000 California residents must establish, document, and comply with a formal training policy (Cal. Code Regs. tit. 11, § 7100(b)).
[14] Cal. Code Regs. tit. 11, § 7151(a).
[15] Mont. Code § 30-14-2801(2)(b).
[16] 4 Colo. Code Regs. § 904-3:8.05(E).
[17] Cal. Code Regs. tit. 11, § 7155(b).
[18] Cal. Code Regs. tit. 11, § 7101(a); 4 Colo. Code Regs. § 904-3:6.11(A).
[19] 4 Colo. Code Regs. § 904-3:6.11(D).
[20] Del. Code tit. 6, § 12D-106(a)(11).

including how to respond to resident inquiries about their information. For owners with properties in multiple states, consider adopting the most restrictive standard (Colorado's enumerated factors) as a baseline. Owners operating in Tennessee should evaluate alignment with the National Institute of Standards and Technology (NIST) Privacy Framework to potentially benefit from the statutory affirmative defense. Conduct annual reviews of your security practices and document all policies in a central location accessible to relevant personnel.

Processing Conditions and Prohibitions

U.S. State Comprehensive Consumer Privacy Law expressly prohibits or restricts processing several categories of personal data. "***Targeted Advertising***," sale of personal data, and Profiling for Significant Decisions directed at minors are prohibited where the Controller has actual knowledge (or willfully disregards) that the Data Subject is a minor, with age thresholds varying by state (from ages 16-18). Certain jurisdictions also prohibit the use of geofencing near mental health or reproductive health facilities to track Data Subjects or collect health data. Additionally, the sale of sensitive personal data is banned in several states, though some allow it with the Data Subject's affirmative consent.

Sensitive data categories typically include health information, biometric identifiers, precise geolocation, and data concerning minors, and are subject to heightened protections. Most states require affirmative opt-in consent before collecting or processing sensitive data. Maryland takes a distinct approach, prohibiting the collection or use of sensitive data unless it is "strictly necessary" to provide or maintain a requested product or service, with no exception for consent. For children's data, parental or guardian consent is required across virtually all jurisdictions when the Controller has actual knowledge the Data Subject is under 13.

Controllers must also abide by several "principles" that govern the processing of personal data:

- **Data Minimization**: Limit the collection, use, disclosure, and retention of personal data to the minimum amount that is adequate, relevant, proportionate, and reasonably necessary for the specific purpose(s) for which the personal data is processed, as disclosed to the Data Subject. Specifically, a Controller may not collect, process, or disclose "sensitive" personal data unless it is "strictly necessary" to provide or maintain a specific product or service required by the Data Subject to whom the personal data relates.

- **Purpose Specification** (Avoidance of Secondary Use): Do not collect, use, retain, or disclose personal data in a manner that is not reasonably necessary for, proportionate to, and compatible with both (i) the processing purpose(s) originally specified to the Data Subject at the time of collection and (ii) the processing context, each as they existed at the time of collection, without the Data Subject's consent.

- **Prohibition on Illegal Discrimination**: Do not process personal data in violation of state or federal laws that prohibit unlawful discrimination against individuals.

- **Non-retaliation**: Do not retaliate against a Data Subject for exercising any of the Data Subject Rights afforded to the Data Subject by Applicable Data Protection Law, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the Data Subject, except as expressly permitted by Applicable Data Protection Law.

Practical Implementation Guidance

Apartment owners should audit current data practices against these principles. For data minimization, collect only information necessary for tenancy. Avoid requesting excessive personal details on applications beyond what is needed for credit checks and lease administration. Limit retention of former resident records to the period required by state landlord-tenant laws, then securely dispose of them. When sharing resident data with Third Parties such as marketing partners, ensure the disclosure serves a legitimate purpose disclosed to the resident. Never retaliate against residents who exercise privacy rights. For example, do not refuse to renew a lease or increase rent because a resident requested deletion of their data. If you use screening services that profile prospective residents, ensure the profiling does not result in unlawful discrimination based on protected characteristics. Document the business justification for each category of personal data collected and each Third Party to whom data is disclosed.

Risk Assessment

Privacy Impact Assessment

A Privacy Impact Assessment (**PIA**) identifies, evaluates, and documents mitigations to threats creating privacy risk. A Controller is obligated to conduct a PIA prior to a number of processing activities:

- Engaging in Targeted Advertising.
- Selling personal data.
- Processing "sensitive" personal data.
- Processing the personal data of a Data Subject the Controller has actual knowledge, or willfully disregards, is a minor.
- "**Profiling**"[21] that presents a reasonably foreseeable risk of unfair[22] or deceptive[23] treatment.
- "Profiling" that presents a reasonably foreseeable risk of unlawful disparate impact.[24]

---

[21] "Profiling" is defined as "using automated means to evaluate, analyze, or predict personal aspects concerning a Consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

[22] Under Section 45(n) of the FTC Act, the FTC may rule an act or practice unlawful due to unfairness only if: 1) it causes or is likely to cause substantial injury to consumers, 2) the injury caused is not reasonably avoidable by consumers themselves, 3) the injury caused is not outweighed by countervailing benefits to consumers or to competition.

[23] The FTC has clarified in guidance that an act or practice is to be considered deceptive if it involves a material "representation, omission, or practice that is likely to mislead [a] consumer" who is "acting reasonably in the circumstances."

[24] Disparate-impact discrimination occurs when a seemingly neutral policy or action causes a disproportionate and unjustified negative harm to a group, regardless of intent. Court opinions and agency regulations have applied the disparate-impact theory to discrimination under Title VII of the Civil Rights Act of 1964, age discrimination under the Age Discrimination in Employment Act, lending discrimination under the Equal Credit Opportunity Act, and housing discrimination under the Fair Housing Act (FHA).

- “Profiling” that presents a reasonably foreseeable risk of financial, physical, or reputational injury.[25]

- “Profiling” that presents a reasonably foreseeable risk of a privacy tort (physical or other intrusion upon the solitude or seclusion,[26] or the private affairs or concerns, of a Data Subject that would be offensive to the reasonable person).

- “Profiling” based on data obtained by systematically observing someone in their capacity as an educational program applicant, job applicant, employee, or contractor or based on their presence at a sensitive location.

- “Profiling” that presents a reasonably foreseeable risk of a substantial injury.

- Using, or training, ADMT in connection with certain Significant Decisions.

[25] A long-standing rule in defamation law is that certain defamatory falsehoods—such as the claim that someone has a sexually transmitted disease—warrant the recovery of damages without evidentiary proof. Mike Steenson, Presumed Damages in Defamation Law, 40 Wm. Mitchell L. Rev. 1492, 1492 (2014) (“Despite heavy criticism, the presumed damages rule has had remarkable staying power in American law.”)

[26] Restatement (Second) of Torts § 652B (1977) “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”

The PIA must document:

- **The Processing Context**: What personal data is being collected, whether it is “sensitive,” why it is being collected, the source of the personal data, relationship with Data Subject, what the reasonable expectation of the Data Subject is, etc.
- **Processing Benefits**: The benefits may flow directly and indirectly, to the Controller, Data Subject, other stakeholders, and the public.
- **Potential Harms**: The potential harms to the privacy or rights of the Data Subject the processing creates or makes more likely. Applicable regulations require the consideration of constitutional, intellectual privacy, data security, discrimination, unfair or deceptive acts or practices, adverse Significant Decisions, and financial, physical, and psychological harms. What is the source of the harm and the cause?
- **Safeguards**: The controls that have been put in place to mitigate the risk of harm?
- **Evaluation**: The benefits must be weighed against the mitigated risk of harm.

Notably, California expressly requires the assessment to be conducted "prior to" engaging in the processing activity; other states do not specify timing with the same precision.

Practical Implementation Guidance

Identify processing activities requiring a PIA. This is most commonly using any screening service that doesn’t qualify as a “credit reporting agency” under the FCRA, Targeted Advertising to prospective renters, and any profiling that affects housing decisions. Develop a standardized PIA template addressing the required elements: what data is collected, from whom, why, the benefits of processing, potential harm (particularly discrimination or denial of housing), and safeguards in place. Conduct the PIA before launching any new screening tool or advertising program that uses resident data. If you use automated resident screening that makes or substantially influences rental decisions, assess whether the technology meets the ADMT threshold and document how human review is incorporated. Retain completed PIAs for at least five years following California’s standard. For multi-property owners, establish a centralized PIA workflow triggered whenever a new vendor relationship or technology tool is introduced that involves resident personal data.

Public Disclosures

U.S. State Comprehensive Consumer Privacy Law requires Controllers to make up to seven kinds of public disclosures. The four types of public disclosures relevant to most apartment owners are discussed below.[27]

Privacy Notice

A "Privacy Notice"[28] is a public advisement, often on a website, containing statutorily required disclosures describing how a Controller processes personal data, both online and offline. The specific requirements vary by jurisdiction, but all jurisdictions require the Privacy Notice to describe the categories of personal data collected, including whether sensitive personal data or children's personal data is processed, the sources from which that data is collected, and the specific purposes for which the data is processed in addition to instructions on how Data Subjects may exercise their rights. Many jurisdictions require additional information, such as the categories of Third-Parties the Controller discloses personal data to, the categories of personal data, and the purpose, whether personal data will be "sold," and under Connecticut law specifically whether it will be used to train large language models, etc.

Notice at Collection

The "Notice at Collection" is a unique California requirement. In addition to a Privacy Notice, the CCPA requires a "Notice at Collection," which is a form of "just in time" notice that "at or before the point of collection" provides Data Subjects with notice of the categories of personal information to be collected, the purpose for which each category of information is used, whether that information will be "sold" or "shared," and how long it will be retained.[29] While a Controller may have many "Notices at Collection," these notices roll up to one "Privacy Policy."[30]

In one enforcement action, the California Attorney General faulted a platform for virtual health services that also had a separate public-facing website collecting information subject to the CCPA for merely linking to its "Privacy Policy" rather than "deep-linking" to send Data Subjects to the relevant portion of the Privacy Notice containing the Notice at Collection.[31]

---

[27] Three less-relevant public disclosures concern loyalty programs, collection of biometric identifiers, and use of facial recognition technology: California and Colorado require specific notices when offering loyalty programs, Colorado requires a specific notice when collecting biometric identifiers, Connecticut requires a specific notice when using facial recognition technology.

[28] Calling these disclosures "notices" instead of "policies" clarifies that the document is a public, external communication intended for users, customers, or regulators, rather than an internal company document. While a policy dictates internal procedures, a notice directly informs users about the collection, use, disclosure, and retention of their personal data, aligning with legal transparency requirements.

[29] Cal. Code Regs. tit. 11, § 7012.

[30] As evidence of the distinction between a "Notice at Collection" and "Privacy Policy" under the CCPA, consider that one of the required elements of a "Notice at Collection" is that it include "a link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online." (Cal. Code Regs. tit. 11, § 7012(e)(6).

[31] California Attorney General, "CCPA Enforcement Case Examples," "A business that provides a platform for virtual healthcare services also had a separate public-facing website that collected personal information and is subject to the CCPA. The business's link to its notice at collection sent

Adverse Action Notice

Amendments revising the Delaware Personal Data Privacy Act in 2026 introduced novel obligations regulating data that doesn't meet the legal definition of a "consumer report" under the FCRA.[32] Under these requirements, if an entity uses personal data disclosed by a Third-Party that is not a "consumer report" under the FCRA (a **report**) to make a Significant Decision, including any recommendations, summaries, or automated decisions, and the entity takes an "Adverse Action,"[33] the entity must provide an Adverse Action Notice to the individual. Notably, the contractual and notice obligations imposed by these amendments expressly apply to individuals in their commercial or employment context, in addition to individuals acting in their individual, personal, or household context.

Automated Decision-Making Technology Notice

An additional unique California requirement relates to the use of ADMT to make a Significant Decision. A Controller must provide an ADMT Notice either at or before the point of collecting personal information it plans to process using ADMT, or before repurposing previously collected data for ADMT use. The notice must include a plain language explanation of: (1) the specific purpose for using ADMT; (2) how the ADMT processes personal information to reach a Significant Decision, including the categories of personal information that affect the output; (3) the type of output generated (e.g., scores, recommendations); and (4) how that output factors into the decision. It must also describe the Data Subject's right to opt out of ADMT (or the applicable exception, such as a human-reviewer appeal process), the right to access ADMT information, instructions for submitting opt-out or appeal requests, and a non-retaliation disclaimer.

Practical Implementation Guidance

Develop a comprehensive privacy notice for your website and leasing office that discloses the categories of personal data collected (application information, payment records, maintenance history), the purposes for collection, and the Third Parties with whom data is shared. For California properties, implement "just in time" notices at collection—for example, a brief disclosure on online application forms before residents submit personal information, with a deep link to the full privacy policy. Review privacy notices annually and update them as practices change. If you use automated decision-making tools for rental decisions and operate in California, prepare an

---

consumers to the beginning of its privacy policy instead of the relevant section. The business's privacy policy also failed to describe the information a consumer must provide in order to make a verifiable consumer request, list the categories of personal information collected or disclosed in the past twelve months, and list the categories of third parties for each category of personal information disclosed for a business purpose. After being notified of alleged noncompliance, the business made its notice readily available to consumers by "deep-linking" to send consumers to the relevant section of its privacy policy and updated its privacy policy to include the required disclosures. (available at https://oag.ca.gov/privacy/ccpa/enforcement).

[32] 15 U.S.C. §§ 1681–1681x) and implementing regulations promulgated at 12 C.F.R. § 1022.

[33] "Adverse action" means any denial, cancellation, unfavorable change, increase in charge, exclusion of benefit, or other action adverse to the interests of a consumer or resident in connection with a Significant Decision.

ADMT-specific notice explaining how the technology works and how residents can request human review. For Delaware properties, establish a process to provide adverse action notices when denying applications based on Third-Party data that isn't considered a "consumer report" under the FCRA, including a description of the data relied upon and instructions for requesting human review.

Contractual Requirements

A data processing agreement/addendum (**DPA**) is used “to document a set of instructions and memorialize data protection obligations between two parties that are planning to send and receive personal data between themselves for specified purposes.”[34] Required provisions vary depending on whether the recipient is a Processor or a Third Party.

Processors

Under U.S. State Comprehensive Consumer Privacy Laws, a contract that meets specific statutory requirements is essential for an entity to qualify as a Processor (or, in California, a "service provider" or "contractor") rather than being treated as an independent Controller (or Third Party). There are several interrelated reasons why this contractual compliance matters.

- In California, the written contract is a definitional prerequisite. Under the CCPA, a "service provider" is defined as a person that processes personal information on behalf of a business pursuant to a written contract that contains specific prohibitions, including prohibitions on selling or sharing the personal information, using it for purposes beyond the business purposes specified in the contract, and using it outside the direct business relationship.

- Across these laws, whether a person acts as a Controller or Processor is a “fact-based determination” that depends on the context of the processing. A person who "is not limited in the person's processing of personal data pursuant to a Controller's instructions, or that fails to adhere to the instructions, is a Controller and not a Processor." If a Processor "begins, alone or jointly with others, determining the purposes and means of the processing," it becomes a Controller with respect to that processing and may be subject to enforcement action.

- If the recipient is not a Processor as intended, the disclosure may be considered a “sale” under applicable law. This can trigger a number of compliance obligations, such as 1) providing Data Subjects with an opportunity to exercise their Right to Opt-Out of Sale and honoring such requests, 2) updating the privacy notice with specific disclosures, and 3) conducting and documenting a PIA.

The DPA is required to contain a number of provisions, including:

- **Processing scope**: Instructions for processing, the nature and purpose of processing, the types of personal data to be processed, and the duration of processing.

- **Rights and obligations**: A clear statement of each party's rights and obligations.

- **Confidentiality**: An obligation on the Processor to ensure each person processing personal data is subject to a duty of confidentiality.

---

[34] Justin Weiss, Data Processing Agreements: Coordination, Drafting & Negotiation (2019), pg. 12.

- **Data deletion/return**: An obligation on the Processor to delete or return all personal data at the Controller's direction upon termination of services, unless retention is required by law.
- **Compliance demonstration**: An obligation on the Processor to make available all information necessary to demonstrate compliance with applicable law.
- **Controller oversight/audit**: The Processor must either allow reasonable assessments by the Controller or engage a qualified, independent assessor to audit its policies and technical/organizational measures.
- **Subprocessor controls**: A requirement that subprocessors be engaged only under a written contract imposing obligations no less protective than those on the Processor.
- **Security measures**: Some states (notably Colorado, Maryland, Minnesota, and New Jersey) specifically require the contract to impose reasonable technical and organizational security measures on the Processor.

Third Parties

California and Delaware have unique requirements when disclosing personal data to a Third Party. Under both statutes, the contract must limit the disclosure of personal data to specified purposes, obligate the Third Party to comply with the applicable privacy law and provide the same level of privacy protection it requires, and grant the disclosing party the right to monitor the Third Party's compliance and to stop and remediate any unauthorized use of personal data. The Third Party must also notify the disclosing party if it can no longer meet its obligations.

California additionally requires that purpose descriptions be specific rather than generic and provides illustrative compliance mechanisms such as attestation and honoring forwarded opt-out requests. Delaware imposes additional obligations when personal data is used for Significant Decisions, including requiring the Third-Party to notify residents of adverse actions, describe the data relied upon, inform residents of their access rights, and offer human review of adverse decisions where technically feasible.

Practical Implementation Guidance

Apartment owners should review all vendor contracts involving resident data, particularly agreements with resident screening services, property management software providers, payment processors, maintenance request platforms, and marketing agencies. Ensure each contract includes required DPA provisions: Clear processing instructions, confidentiality obligations, data deletion upon termination, audit rights, and restrictions on secondary use. It is common to have one DPA for use with Processors, and one for use with Third Parties, each containing the most restrictive terms required by U.S. law for that kind of relationship so that it may be used in every jurisdiction. For Processors, verify the contract prohibits using resident data beyond providing the contracted services. For Third Parties (such as marketing partners receiving resident data), ensure contracts limit use to specified purposes and grant you the right to monitor compliance. In addition to terms required by US Comprehensive Consumer Privacy Law, consider provisions responsive to U.S. data breach notification law, such as when notice of a data breach is required,

what information the counterparty is required to provide, and (if not addressed by the liability provisions of the main agreement) allocation of data breach notification costs.

When onboarding new vendors, include privacy compliance questionnaires in due diligence. For Delaware properties, implement enhanced due diligence for Third-Party disclosures commensurate with data sensitivity. Maintain a vendor inventory documenting each relationship, the data shared, and the applicable contract terms.

Data Subject Right Requests

Available Data Subject Rights

U.S. State Comprehensive Consumer Privacy Laws grant Data Subjects 13 rights. Taking the most restrictive version of the various formulations, they can be described as follows:

- **Right to Verify**: A Data Subject may request that a Controller confirm whether the Controller, or a Processor or Third Party acting on the Controller's behalf, is processing or has processed their personal data.
- **Right to Access**: A Data Subject may request that a Controller give the Data Subject access to their personal data.
- **Right to Correct**: A Data Subject may request that a Controller that maintains inaccurate personal data correct inaccuracies in the Data Subject's personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data.
- **Right to Delete**: A Data Subject may request that a Controller delete personal data provided by, collected from, obtained about, or concerning the Data Subject.
- **Right to Personal Data Portability**: A Data Subject may request that a Controller disclose a copy of the Data Subject's personal data to the Data Subject in a portable and, to the extent technically feasible, readily usable format that allows the Data Subject to transmit the data to another person without hindrance.
- **Right to Opt-Out of Sale**: A Data Subject may request that a Controller cease collecting, using, and disclosing their personal data for the purpose of disclosing their personal data to a Third Party for monetary or other valuable consideration.
- **Right to Opt-Out of Targeted Advertising**: A Data Subject may request that a Controller cease collecting, using, and disclosing their personal data for the purpose of displaying an advertisement to the Data Subject or on a device identified by a unique identifier that is selected based on personal data obtained or inferred over time from the Data Subject's activities across nonaffiliated websites or applications to predict the Data Subject's preferences or interests.
- **Right to Know Categories of Third-Parties Receiving Personal Data**: A Data Subject may request that a Controller provide the Data Subject with a list of the categories of Third Parties to whom the Controller has disclosed the Data Subject's personal data.
- **Right to Know Specific Third Parties Receiving Personal Data**: A Data Subject may request that a Controller disclose to the Data Subject the Third Parties to whom the Controller has disclosed the Data Subject's personal data, or (in the alternative) any Data Subject's personal data.

- **Right to Limit the Use and Disclosure of Sensitive Personal Data**: A Data Subject may request that a Controller using and disclosing the Data Subject's personal data to infer characteristics about the Data Subject for a purpose other than the following purposes cease using and disclosing their "sensitive" personal data for any purpose except for the following purposes: 1) to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, 2) to prevent, detect, and investigate security incidents, 3) short-term, transient use, 4) to conduct internal business operations, 5) to verify or maintain, or improve, upgrade, or enhance, the quality or safety of a product, service, or device, 6) fraud prevention, detection, or prosecution, and 7) to ensure the physical safety of natural persons.

- **Right to Opt-Out of Profiling for Significant Decisions**: A Data Subject may request that a Controller cease collecting, using, and disclosing their personal data for the purpose of using automated means to evaluate, analyze, or predict personal aspects concerning a Data Subject's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements in furtherance of a decision that results in the provision or denial of 1) financial or lending services, 2) housing, 3) insurance, 4) education enrollment or opportunity, 5) criminal justice, 6) employment opportunities, 7) health-care services, 8) access to essential goods or services, or 9) basic necessities, such as food and water.

- **Right to Review Significant Decisions Based on Profiling**: A Data Subject may request that a Controller collecting, using, and disclosing their personal data for the purpose of using automated means to evaluate, analyze, or predict personal aspects concerning a Data Subject's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, or health-care services permit the Data Subject to 1) review personal data collected, used, and disclosed for the purpose of automatically evaluating, analyzing, or predicting of the Data Subject's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements in furtherance of the automated decision, 2) question the results of the automated evaluation, analysis, or prediction of the Data Subject's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements, 3) (if feasible) be informed of the reason why the automated evaluation, analysis, or prediction resulted in the automated decision, and 4) allow the Data Subject to correct any incorrect personal data that were collected, used, and disclosed for the purposes of the automated decision and have the decision reevaluated based on the corrected personal data.

- **California Right to Know**: A Data Subject may request that a Controller disclose 1) the categories of personal data the Controller has collected about the Data Subject, 2) the specific pieces of personal data the Controller has collected about the Data Subject (except for "highly sensitive identifiers"), 3) the categories of sources from which the personal data was collected, 4) the "business purpose" or "commercial purpose" for collecting the personal data, 5) the categories of personal data disclosed for a "business purpose," 6) the categories of Service Providers and Contractors to whom the Controller has disclosed the Data Subject's personal data for a "business purpose," 7) the categories of Third Parties to whom the Controller has disclosed the Data Subject's personal data for a "business purpose," 8) the categories of Third Parties to whom the Controller has "sold" or "shared" the Data Subject's personal data, 9) the

categories of personal data that the Controller "sold" or "shared" to each category of Third-Party, and 10) the "business purpose" or "commercial purpose" for "selling" or "sharing" the personal data in the last 12 months (or from as far back as January 1, 2022, if requested by the Data Subject).

Figure 7 provides an overview of which rights are available in which jurisdictions.[35]

[35] For ease of comparison to other jurisdictions, this guidance document combines the Right of Access/ Verification and breaks the California "Right to Know" into the Right of Access, the Right to Verify, the Right to Personal Data Portability, and the Right to Know Categories of "Third-Parties" Receiving Personal Data for purposes of the comparison table.

State	Access / Verification	Correction	Deletion	Opt-Out of Processing For…			Personal Data Portability	Categories of Third Parties Receiving Personal Data	Specific Third Parties Receiving Personal Data	Limit use and disclosure of Sensitive Personal Data	Review of Significant Decisions Based on Profiling
				Targeted Advertising	Sale	Profiling for Significant Decisions					
AL	X	X	X	X	X	X	X				
CA	X	X	X	X	X		X	X		X	
CO	X	X	X	X	X	X	X				
CT	X	X	X	X	X	X	X		X		X
DE	X	X	X	X	X	X	X		X		
IA	X	X	X		X		X				
IN	X	X	X	X	X	X	X				
KY	X	X	X	X	X	X	X				
LA	X	X	X	X	X	X	X				
MD	X	X	X	X	X	X	X	X			
MN	X	X	X	X	X	X	X		X		X
MT	X	X	X	X	X	X	X				

State	Access / Verification	Correction	Deletion	Opt-Out of Processing For…			Personal Data Portability	Categories of Third Parties Receiving Personal Data	Specific Third Parties Receiving Personal Data	Limit use and disclosure of Sensitive Personal Data	Review of Significant Decisions Based on Profiling
				Targeted Advertising	Sale	Profiling for Significant Decisions					
NE	X	X	X	X	X	X	X				
NH	X	X	X	X	X	X	X				
NJ	X	X	X	X	X	X	X				
OK	X	X	X	X	X	X	X				
OR	X	X	X	X	X	X	X		X		
RI	X	X	X	X	X	X	X				
TN	X	X	X	X	X	X	X				
TX	X	X	X	X	X	X	X				
UT	X	X	X	X	X		X				
VA	X	X	X	X	X	X					
VT	X	X	X	X	X	X	X		X		X

Figure 7: Data Subject Rights by Jurisdiction as of October 2026

Intake of Data Subject Right Requests

Required Intake Channels

A Controller must provide at least two Data Subject Right Request mechanisms.[36] Acceptable mechanisms include a dedicated email address, toll-free telephone number, digital webform, in-person form, or mail submission. Notably, a cookie banner or consent management platform does not qualify as an acceptable intake method for opt-out requests because it concerns data collection rather than the sale or sharing of personal data. Controllers with websites or mobile applications must provide a toll-free telephone number; those operating exclusively online with a direct consumer relationship may provide only an email address. Controllers must additionally accept opt-out requests via an Opt-Out Preference Signal (**OOPS**), such as the Global Privacy Control, which has been endorsed by the California Privacy Protection Agency, Connecticut Attorney General, and Colorado Attorney General, among others. Mechanisms must be easy to understand, easy to use, require minimal steps, maintain "symmetry in choice," and avoid confusing language or dark patterns.

Authentication at Intake

A Controller must establish, document, and comply with a reasonable authentication method for verifying the identity of a requestor. Authentication may be accomplished through existing password-protected account practices or by either using a Third-Party identity verification service or matching identifying information already maintained by the Controller. Controllers must not collect "highly sensitive identifiers" — such as Social Security numbers, financial account numbers, or biometric data — unless necessary for authentication. Authentication mechanisms must be commercially reasonable, must consider the type and sensitivity of the data at issue, the risk of harm from unauthorized access, and the likelihood of fraudulent actors. Controllers may not charge a fee for authentication.

Authorized Agents

Authorized agents—including natural persons, legal persons, and in certain jurisdictions "technology" mechanisms—may submit requests on behalf of Data Subjects, with permissible agent types varying by state. California distinguishes between natural and legal persons; Colorado, Connecticut, Minnesota, Montana, New Hampshire, New Jersey, and others recognize both, while some states are silent. For adults generally, authorized agents are typically limited to opt-out rights, whereas for children and adults under protective arrangements, agents may exercise all rights in most jurisdictions. A Controller may require the agent to provide the Data Subject's signed permission demonstrating authorization and may also require the Data Subject to

[36] Colorado requires two mechanisms only where the Controller interacts with Data Subjects beyond online channels; Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, New Hampshire, Oregon, Rhode Island, Tennessee, Utah, and Virginia require only one mechanism.

independently authenticate their identity or confirm the agent's designation—unless the agent holds a power of attorney.

Evaluating Data Subject Right Requests

Authentication Requirements by Right

Whether authentication is required, permitted, or prohibited depends on the specific right and the jurisdiction. Rights to Correct, Delete, and California's Right to Know **require** authentication. Rights to Verify, Access, and Personal Data Portability **permit** but do not mandate authentication. In contrast, authentication is **prohibited** for the Right to Opt-Out of Sale and the Right to Opt-Out of Targeted Advertising in California and Oregon, and Right to Limit Use and Disclosure of Sensitive Personal Data in California.

Universal Bases for Denial

Across jurisdictions, a Controller may deny a request on the following grounds: (1) inability to authenticate the requestor's identity using commercially reasonable efforts; (2) a good-faith, reasonable, and documented belief that the request is fraudulent; and (3) where an authorized agent fails to provide the Data Subject's signed permission. Most jurisdictions additionally permit denial where requests are manifestly unfounded or excessive and repetitive, though Colorado and Oregon do not recognize these grounds. Certain jurisdictions also permit denial for technical infeasibility (Iowa, Kentucky, Maryland, Montana, Utah) or where the request harasses or imposes undue burden (Utah).

Determining Scope and Reach

Scope restrictions can be characterized by three parameters: **Limitations** (restrictions embedded within the right's statutory text), **exceptions** (right-specific carve-outs to otherwise valid requests), and **exclusions** (processing purposes placed entirely outside the reach of any right). Exclusions permit a Controller to limit effectuation to comply with federal, state, or local law; to cooperate with civil, criminal, or regulatory investigations; and to exercise or defend legal claims. For deletion specifically, a Controller may retain data necessary to complete a transaction, for legal compliance, or for internal uses reasonably aligned with Data Subject expectations. Controllers must also identify data that may not be disclosed in access responses such as highly sensitive identifiers and consider trade-secret limitations applicable in certain states.

Responding to Data Subject Right Requests

Response Timelines

The general response deadline is **45 calendar days** from receipt, with an available **45-day extension** upon providing the Data Subject with a Notice of Extension explaining the reasons for the delay within the initial 45 days. Iowa is the principal exception, granting 90 days for initial response with a 45-day extension (maximum 135 days). For opt-out requests (sale and Targeted Advertising), denial notices must be issued within **15 days** in most jurisdictions. California requires a **Notice of Receipt** within **10 business days** for Right to Know, Right to Correct, and Right to Delete requests, which must describe the authentication process and expected response timeline. For appeals, most states allow 60 days without extension; Colorado and Minnesota require a response within 45 days but permit a 60-day extension; Oregon and New Jersey allow 45 days with no extension. Figure 8 provides the most restrictive timelines to provide notice of receipt, effectuate the request, provide notice of the need of an extension, and provide notice of denial.

Right	Notice of Receipt	Effectuation (most restrictive)	Extension	Denial Notice
Verify	None	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
Access	None	45 days; 90 with extension	Notice within first 45 days	45 days
Correct	10 business days (California)	45 days; 90 with extension	Notice with reasons within first 45 days	45 calendar days
Delete	10 business days (California)	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
Personal Data Portability	None	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
Opt-Out of Sale	None	15 business days. Opt-out preference signals: as soon as feasible, including immediately	Not permitted in California	15 days (adjusted for California)
Opt-Out of Targeted Advertising	None	15 business days. Opt-out preference signals: as soon as feasible	Not permitted in California	15 days (adjusted for California)

Know Categories of Third Parties (Maryland)	None	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
Know Specific Third Parties	None	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
Limit Use of Sensitive Personal Data	None	15 business days	Not permitted in California	15 business days
Opt-Out of Profiling for Significant Decisions	None	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
Review Significant Decisions Based on Profiling	None	45 days; 90 with extension	Notice with reasons within first 45 days	45 days
California Right to Know	10 business days	45 days	Notice with reasons within first 45 days	45 days

Figure 8: Data Subject Rights Timeline Comparison

Template Responses

Many businesses develop and use a set of vetted communication templates when effectuating Data Subject Right requests. Common template communications include:

- **Notice of Receipt** (California): Must confirm receipt, describe the authentication process, and state when the Data Subject should expect a response; may be given in the same manner the request was received.
- **Notice of Decision — Denial**: Must include the grounds for denial and instructions **on** how to appeal the decision with the Controller. Where a Right to Correct is denied and the data can be deleted, the notice must inform the Data Subject of their Right to Delete and provide instructions.

- **Notice of Decision — Fulfillment**: Must inform the Data Subject of any action taken in response to the request. For deletion, the notice must state that the request has been effectuated and that a record will be maintained per regulatory requirements. For access requests, the response must be concise, transparent, in a commonly used electronic format, in the Data Subject's language, and free of incomprehensible internal codes.

- **Notice of Extension**: Must state the reasons for the delay and the length of the extension and be delivered within the initial 45-day window.

- **Third-Party Notifications**: Where a Controller cannot notify all Third Parties to whom it has sold or shared personal data of the need to delete, it must provide the Data Subject a detailed explanation of why such notification is impossible or would involve disproportionate effort.

Appeals

When a Controller denies a Data Subject rights request, it generally must include instructions for how the Data Subject can appeal the decision. The appeal is directed to the Controller itself, not to a regulatory authority in the first instance.

- **Timelines for appeal responses** vary by jurisdiction. Most states — including Connecticut, Delaware, Iowa, Indiana, Kentucky, Maryland, Montana, Nebraska, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, and Virginia—allow **60 days** to respond to an appeal with no extension. Colorado and Minnesota require a response within **45 days** but permit a **60-day extension**. Oregon and New Jersey allow **45 days** with no extension.

- **Required content** of the appeal disposition includes a written explanation of any action taken or not taken, the reasons for the decision, and—critically—information about the Data Subject's ability to **contact the Attorney General** if they have concerns about the outcome. These content requirements apply whether the Controller reverses or upholds the original denial.

Practical Implementation Guidance

Establish clear intake mechanisms for Data Subject Right Requests. At minimum, this likely requires a dedicated email address and a webform on the property website. Train leasing office staff to recognize and promptly route privacy requests . Develop a verification process that confirms requestor identity without collecting excessive information, matching name and unit number against lease records typically suffices. Create template responses for common scenarios: Acknowledgment of receipt (within 10 business days for California), fulfillment notices, denial notices with appeal instructions, and extension notices when more time is needed. Respond within 45 days, using the 45-day extension only when genuinely necessary. For opt-out requests regarding sale or Targeted Advertising, respond within 15 days and honor Global Privacy Control signals if detected. Document all requests and responses for at least 24 months. When denying requests, always include instructions for appeal and, if the appeal is denied, information about contacting the state Attorney General.

Glossary

This glossary contains composite definitions amalgamated from the most restrictive elements of comparable terms across all 23 of the U.S. State Comprehensive Consumer Privacy Laws.

- **Anonymized Data**: Information that was previously personal data that has been modified using irreversible statistical disclosure limitation techniques or methods so that the information can no longer reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable Data Subject or a device linked to such individual.

- **Controller:** Used to mean the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data, and that surpasses the jurisdictional threshold for a given comprehensive consumer privacy law without an applicable data or entity exemption.

- **Data Subject**: The identified or identifiable natural person to whom the personal data relates.

- **De-identified Data:** Anonymized Data where the Controller has 1) implemented reasonable administrative and technical measures to ensure that the data cannot be re-associated with a Data Subject, 2) publicly committed to Process the data as Anonymized Data and not attempt to re-identify it, and 3) contractually obligated any recipients of the data to comply with the requirements of applicable data protection law regarding "de-identified data," including by not attempting to re-identify the data.

- **Personal Data:** Information or data that identifies, is linked with, relates to, describes, or could reasonably be linked or associated, directly or indirectly, with an identified or identifiable Data Subject or a device that identifies, is linked to, or is reasonably linkable to one or more Data Subjects in a household.

- **Process:** Any operation or set of operations performed on information, whether or not by automatic means, including creating, collecting, receiving, accessing, modifying, storing, using, disclosing, making available, and destroying the information.

- **Processor:** A natural or legal entity that processes personal data on behalf of a Controller.

- **Pseudonymous Data:** Personal data that can no longer be attributed to a specific Data Subject without the use of additional information, provided that the additional information 1) is kept separately and 2) is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

- **Significant Decision:** Decisions made by the Controller that result in the provision or denial by the Controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

- **Targeted Advertising:** Displaying an advertisement to a Data Subject, or on a device identified by a unique identifier, where the advertisement is selected based on personal data obtained or inferred over time from the Data Subject's activities over time across nonaffiliated websites, applications, or online services other than the business, distinctly branded internet website, application, or service with which the Data Subject intentionally interacts.

- **Third Party:** A person other than the Data Subject, the Controller, or a Processor.

Appendix: Comprehensive Consumer Privacy Law Statutes

- Alabama Personal Data Protection Act (effective May 1, 2027)
- California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act, Cal. Civ. Code §§ 1798.100–199.100; Cal. Code Regs. tit. 11. §§ 7000–7304
- Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301–1313; 4 Colo. Code Regs 904-3
- Connecticut Data Privacy Act, Conn. Gen. Stat. §§ 42-515–527
- Delaware Personal Data Privacy Act, Del. Code tit. 6 §§ 12D-101–111 (amendments effective January 1, 2027)
- Indiana Consumer Data Protection Act, Ind. Code § 24-15
- Iowa Consumer Data Protection Act, Iowa Code §§ 715D.1–715D.9
- Kentucky Consumer Data Protection Act, Ky. Rev. Stat § 367.3611–367.3629
- Louisiana Data Privacy Act, La. Stat. §§ 51:1780.1–5 (effective January 1, 2027)
- Maryland Online Data Privacy Act, Md. Commercial Law Code §§ 14-4701–4714
- Minnesota Consumer Data Privacy Act, Minn. Stat. §§ 325M.10–325M.21
- Montana Consumer Data Privacy Act, Mont. Code §§ 30-14-2801–2817
- Nebraska Data Privacy Act, Neb. Rev. Stat. §§ 87-1101–1130
- New Hampshire Data Privacy Act, N.H. Rev. Stat. §§ 507-H:1–12
- New Jersey Data Privacy Act, N. J. Stat. § 56:8-166; N.J.A.C. 13:45L
- Okla. Stat. tit. 75A, §§ 301–320 (effective January 1, 2027)
- Oregon Consumer Privacy Act, Or. Rev. Stat. §§ 646A.570–646A.589
- Rhode Island Data Transparency and Privacy Protection Act, 6 R.I. Gen. Laws §§ 6-48.1-1–10
- Tennessee Information Protection Act, Tenn. Code §§ 47-18-3301–3315
- Texas Data Privacy and Security Act, Tex. Bus. & Com. Code §§ 541.001–107
- Utah Consumer Privacy Act, Utah Code §§ 13-61-101–404
- Vermont Data Privacy and Online Surveillance Act, Vt. Stat. tit. 9, § 2415a–2415k (effective January 1, 2028)
- Virginia Consumer Data Protection Act, Va. Code §§ 59.1-575–584

Privacy law in the U.S. is complex. Let Dentons simplify it for you.

DENTONS

Scan the QR code to access Dentons' **Comprehensive Consumer Privacy Law Threshold Assessment** and receive a complimentary report detailing which of the U.S. Comprehensive Consumer Privacy Laws may be within scope for your organization.

NAA LEGAL AFFAIRS

© 2026 Dentons.

Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for legal notices.