2025 DATA PRIVACY RISK SNAPSHOT FOR MULTIFAMILY OPERATORS

October 2025

The Current Landscape

2025 is shaping up to be another landmark year for data privacy legislation in the United States. States continue to adopt comprehensive consumer data privacy laws modeled after California's California Consumer Privacy Act (CCPA), expanding protections across the country.

As of late 2025, 19 U.S. states have signed comprehensive data privacy laws, including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia.

Most of these laws grant consumers familiar rights — such as the ability to access, delete and opt out of the sale of their personal data — and require businesses to maintain transparent privacy policies. However, the specific thresholds, definitions and enforcement mechanisms vary by state.

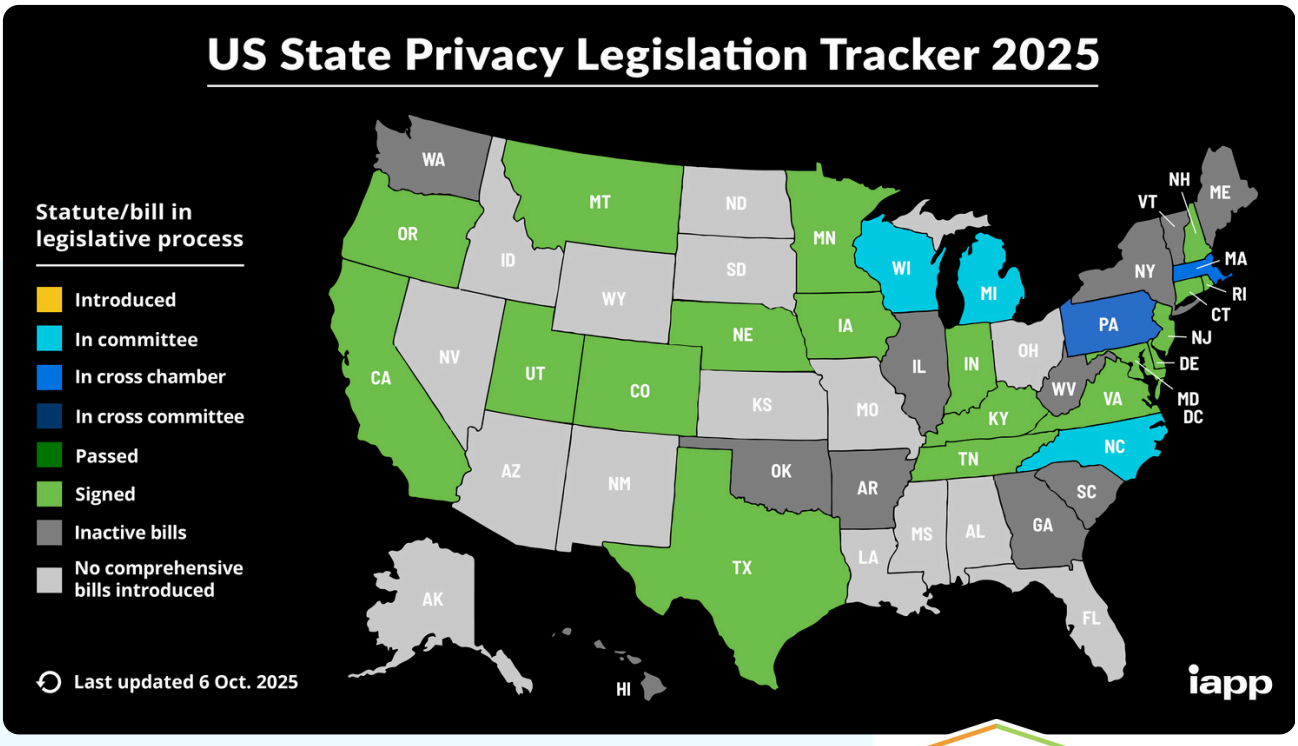
The Maryland Online Data Privacy Act (MODPA) is among the latest to take effect, officially becoming enforceable on October 1, 2025. It applies to companies processing the personal data of at least 35,000 Maryland residents annually, or 10,000 residents if more than 20% of the company's revenue comes from selling personal data.

While the law's effective date is October 1, 2025, it does not apply retroactively to data processing activities that occurred before April 1, 2026.

Rhode Island became the 19th state to enact a comprehensive data privacy law, which takes effect on January 1, 2026. The law requires companies to obtain consent before processing sensitive personal data. However, it has drawn criticism from privacy advocates who argue that its provisions do not meaningfully restrict how companies collect or use personal information.

Several other states — including Massachusetts, Michigan, North Carolina, Pennsylvania, and Wisconsin — currently have active privacy bills under legislative consideration, signaling that the state-by-state trend toward comprehensive privacy regulation is likely to continue in 2026 and beyond.

For ongoing updates and comparisons, the International Association of Privacy Professionals (IAPP) maintains an excellent resource: the U.S. State Privacy Legislation Tracker.



Expert Q&A with Lisa Angelo, Esq.

To get a fresh take on the risks facing multifamily operators, the WithMe team recently spoke with nationally recognized cyber liability expert Lisa Angelo, Esq.

What's the outlook for more states, and even the federal government, passing legislation similar to what has been enacted in California?

Since the CCPA was established in January 2020, many states have enacted similar laws, with a lot of progress in 2025.

What are the distinct buckets of risk facing operators when it comes to resident documents stored on their systems?

The risk falls into three distinct buckets, each with their own set of financial, oversight and reputational risks.

Risk of data breach.

This is the actual risk of resident data breach, which is defined as having undergone unauthorized access. It's important to note the law is broad on what access is considered unauthorized. This could be an unknown attacker who gained access to your systems, but it could also be a disgruntled current or ex-employee who takes copies of your data or files.

The hard costs of this risk include:

- Civil liability to data breach victims
- Fines to governing bodies, per state statute
- Reputational risk for any breach that is made public

Risk of non-compliance with data privacy laws and provisions.

Some data privacy laws call for businesses that touch consumer data to comply with evolving guidelines, which may feel like a moving target. This is especially true when there is rule-making authority such as the California Privacy Protection Agency ("CPPA"), established by the California Consumer Privacy Act of 2018 ("CCPA").

These laws typically require: transparency about the data processing; consent for various types of processing; and honoring consumers' rights to control their personal information, which may include timely data deletion, data correction and data portability.

The hard costs of non-compliance include:

- Statutory fines per incident. While most state-level enforcement activity comes after a reported data breach, there are avenues for disgruntled consumers to report non-compliance with these laws to the regulators. State privacy regulators can then decide whether or not to investigate a company.

- Legal defense costs for defending against litigation and communicating with regulators who are either investigating or fining your business.

Risk of overstating data security and encryption practices.

Under the FTC Act, the Federal Trade Commission can exercise its authority to prohibit unfair and deceptive practices by taking action against businesses that make misleading security claims (such as being "fully encrypted" or having "state-of-the-art security") if the business fails to deliver on the claims.

When it comes to resident documents being printed, what can operators do to minimize risk?

The best way to minimize risk is to not touch resident data at all. That includes printed documents. On-site property teams will often acquiesce to random requests to print documents, even if their corporate policy is a firm "no." Striking the delicate balance of resident experience and corporate security is tough, and it would be impractical to think that property managers won't ever go rogue.

In lieu of a mere "we will not print for you" policy, building operators can remove their risk by partnering with a third-party company, such as PrintWithMe, to effectively outsource the risk of improper disclosure of personally identifiable information (PII). This risk is at the forefront of data security and legal compliance. It is a type of risk that also carries its own cyber liability insurance policy, which can indemnify the building operator from any of its own risk.

Questions? The WithMe team invites you to connect to discuss data privacy and outsourcing resident and staff printing to PrintWithMe. Email sales@withme.com.

The Compliant & Secure Printing Solution

PrintWithMe is the industry's first secure printing solution for residents and leasing offices, eliminating the risks common to outdated printer systems.

Common Risks	PrintWithMe
User Data and Document Protection	
Resident Password/Email Accounts Hacked Residents often stay signed in and accidentally leave their passwords on key-logging software on common area computers.	**Encrypted Files & Passwords** Certified SSL and TSL ensure data is encrypted. Passwords are stored in our database after being hashed.
Stolen Resident Printouts Residents risk losing important documents if they print without being present at the printer.	**Secure Release Feature for Residents** To prevent the theft or loss of important documents, printing only occurs when the user is physically present at the printer.
Resident Files Hacked Unprotected files are left on public or even staff computers.	**Zero Document Retention** All files are deleted within 24 hours.
Software and Hardware Security Measures	
Data-In-Transit Breach Non-cloud-based printer solutions could have malicious data intermediation.	**No Internal Hard Drive on Printers** Eliminates the risk of documents being stored on the printer.
Outdated Software Vulnerable to Threats Known vulnerabilities in software pose security danger to residents' data and files.	**Regular Software Updates** We regularly apply software patches to production infrastructure to ensure strong security posture.
Internal Operations and Network Protection	
Non-Compliance with Data Privacy Laws Properties or other printing solutions might fail to establish and disclose data practices.	**Fully Compliant with Data Privacy Laws** We maintain transparent data protection practices and honor users' rights to personal data.
Non-Compliance with HIPAA Laws Properties do not identify and protect medical records against reasonably anticipated threats when printing for residents.	**Operational Access Control** We employ multiple authentication mechanisms to reduce the risk of unauthorized access.

WithMe

WITHME.COM

Don’t wait.
Save time and money on your resident and office printing by getting started today.

Email sales@withme.com.