Pennsylvania House Passes Consumer Privacy Bill: What Your Business Needs to Know + 6 Steps You Can Take Now

Insights
10.20.25

Pennsylvania could soon join the growing list of states to enact comprehensive data privacy laws, and businesses that operate in PA must take note. Earlier this month, the commonwealth's House passed a bipartisan consumer privacy bill that would set parameters on the collection and sale of consumers' personal data. We'll explain everything you need to know about HB 78, why it's important, and six steps your business should consider taking now.

Quick Background

Pennsylvania's HB 78, which passed the state's House of Representatives on October 1, would establish the Consumer Data Privacy Act (CDPA) if ultimately approved by the state Senate and Gov. Josh Shapiro. The bill, like its predecessors in other states, is intended to provide consumers with greater control over the collection, use, and sale of personal data. But unlike California's data privacy law, PA's proposed law would **not** cover employment-related information.

Snapshot of the Proposed CDPA

If enacted, the CDPA would establish:

- data privacy rights for consumers;
- duties for "controllers" (for-profit businesses that meet certain conditions, as we explain below);
- duties for "processors" (individuals or entities that process personal data on behalf of a controller); and
- enforcement measures.

The law would become effective one year after its passage.

Covered "Controllers"

The CDPA would apply to any for-profit entity that processes consumers' personal information, does business in Pennsylvania, and meets any one of the following thresholds:

- has annual gross revenue exceeding $10 million;

- annually buys, sells, receives, or shares, for commercial purposes, the personal information of at least 50,000 consumers, households, or devices; or
- derives at least 50% of annual revenues from selling consumers' personal information.

Comparison to Other States. The CDPA's applicability thresholds differ from other states' consumer privacy laws. For example, California has a higher annual gross revenue requirement ($26,625,000 for 2025), and several states have a higher consumer data threshold (100,000 in California, Oregon, and Minnesota).

CDPA Exemptions

The law would provide various important exemptions and carve-outs, including:

- **Exempt Entities.** The following types of entities would **not** be controllers under the CDPA:
  - the Commonwealth or its political subdivisions;
  - non-profit organizations;
  - higher education institutions;
  - national security associations;
  - financial institutions or affiliates subject to Title V of the Gramm-Leach-Bliley Ac; or
  - HIPAA covered entities or business associates.
- **Personal Data Exclusions.** "Personal data" would **not** include publicly available information, de-identified data (subject to the controller meeting certain compliance criteria), or biometric data captured and converted to a mathematical representation.
- **Employment and B2B Data**. Importantly, the CDPA's consumer protections would **not** apply to individuals acting within a commercial or employment context as an employee, owner, director, officer, or contractor.

Comparison to Other States. The CDPA's employment-data exception is consistent with all other state consumer privacy laws, except for the California Consumer Privacy Act (CCPA), which broadly defines "consumer" to include job applicants, current and former employees, and more.

- **Other Exemptions.** Certain types of data, such as protected health information under HIPAA, would be exempt from the CDPA, and limited exceptions would apply to de-identified data and pseudonymous data when certain conditions are met.

Consumer Rights

The CDPA would give various rights to consumers who are Pennsylvania residents, including rights to access, correct, delete, or obtain copies of their personal data processed by a controller.

Consumers also would have certain opt-out rights regarding the use of their data.

Controller Duties

The CDPA would impose significant duties on data controllers, such as:

- **Transparency.** Controllers would be required to provide consumers with a "clear and meaningful" privacy notice that includes the categories of personal data processed by the controller, the purpose of processing personal data, how a consumer can exercise their rights, the categories of personal data shared with third parties (and the categories of each such third party), and an active email address or other online mechanism to contact the controller. Further, data controllers would be required to provide a "clear and conspicuous link" on their websites that enables a consumer to opt out of the targeted advertising or sale of a consumer's personal data.
- **Data Minimization.** Controllers would be limited to collecting personal data that is "adequate, relevant and reasonably necessary" in relation to the disclosed purpose for its collection.
- **Consumer Controls.** Controllers would be required to obtain the consumer's consent before using their personal data for any reason other than the disclosed purpose and before using any "sensitive data" concerning a consumer. Controllers also would be required to provide effective mechanisms for consumers to revoke their consent (which must be at least as easy as it is to provide it) and exercise their opt-out rights. Controllers would have two years to implement opt-out preference signals (OOPS), which allow consumers to automatically opt out of data collection and processing across multiple websites and online services with a single action.

Comparison to Other States. The CDPA's requirement that covered businesses honor OOPS to effect consumers' opt-out rights is on par with at least 12 other states' laws requiring compliance with OOPS and universal opt-out mechanisms (UOOM).

To learn more about OOPS/UOOM, click here (FP insight).

- **Children's Data Privacy.** The CDPA would impose additional restrictions on data related to minor children.
- **Data Protection Assessments.** Controllers would be required to conduct and document a data protection assessment, based on various risks and benefits outlined in the CDPA, for "processing activities that present a heightened risk of harm to a consumer" – which includes certain specified activities, such as the sale of personal data, as well as a broader category for "any other substantial injury to a consumer." (A controller would be deemed to comply with this requirement if it has already conducted a data protection assessment to comply with another state or federal requirement, so long as the assessment is "reasonably similar in scope and effect" to what the CDPA would otherwise require). The state's attorney general would be

authorized to require the controller to disclose an assessment that is relevant to an AG investigation, subject to limited exemptions.

- **Processor Contracts.** Use of third-party data processors are commonplace for companies that have a vast amount of personal data. The CDPA would require controllers to have in place a contract with any processor that "clearly states the instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of ing and rights and obligations of both parties."

Enforcement

Violations of the CDPA would be treated as "unfair methods of competition" and "unfair or deceptive acts or practices" under Pennsylvania's Unfair Trade Practices and Consumer Protection Law. The state's AG would have exclusive enforcement power and the authority to issue regulations under the CDPA.

Although the bill does not include a private right of action or availability of statutory damages, it gives the Pennsylvania Attorney General the ability to initiate enforcement actions. Initially, the AG would be required to, prior to launching an enforcement action, issue a notice of violation to the controller or processor if the AG determines that a cure is possible, and the controller would have an opportunity to cure the violation within 60 days of receiving the notice. However, this requirement would sunset on July 1 in the year after the CDPA took effect.

Comparison to Other States. As it is written currently, the CDPA does not include a private right of action, in line with all existing consumer privacy laws other than the CCPA, which contains a limited private right of action.

What's Next?

A big question remains: will HB 78 suffer the same fate as last year's HB 1201? The 2024 bill also received bipartisan support but ultimately stalled out in the Senate.

This year's HB 78 seems to balance consumer preference while providing safeguards and protections for businesses, which should be appealing to lawmakers on both sides of the aisle. While Governor Shapiro has not commented on the bill, his past actions may indicate his potential support for it. (As Attorney General, Shapiro directed the office to investigate many high-profile data breaches. As governor, he has supported updating data breach notification and security requirements, and he has signed regulations securing insurance data.)

The bill has been transmitted to the Republican-led Senate for consideration, and we'll monitor its progress and provide updates as warranted.

6 Steps Your Business Should Consider Taking Now

While only time will tell whether the CDPA ultimately becomes law, there are plenty of steps your business can take in the meantime to protect itself from data security incidents and privacy-related litigation. Here are six steps you should consider taking now:

- **Evaluate** your organization's current data collection and privacy procedures.
- **Review existing privacy notices and policies**, including those drafted for compliance with the laws of other jurisdictions that have passed similar consumer privacy legislation.
- **Consider engaging in a data mapping exercise**, if your business has not done so recently, to identify consumer data your organization has collected and where that data resides.
- **Identify third parties** with whom your business shares consumer data and any existing data processing agreements with those entities.
- Assess your collection of data concerning **minors** (if any).
- **Stay tuned for updates** and work with data privacy counsel to evaluate your business's readiness for compliance with the CDPA, should it be enacted.

As consumers demand more transparency about who receives their data and what it's used for, and without progress on a federal data privacy scheme, we expect more proposed legislation at the state level, as 19 other states have already enacted similar laws.

Conclusion

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's US Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber team.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Catherine M. Contino
Associate
610.230.6109
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Data Protection and Cybersecurity

Government Relations

Counseling and Advice

Trending

U.S. Privacy Hub

Related Offices

Pittsburgh

Philadelphia