

How Cos. Can Prep For Conn. Data Privacy Amendments

By **William Roberts, Laura Himmelstein and Jacob Buttiker** (April 21, 2026)

Are you a bank using customer data to cross-sell insurance? An auto dealer arranging financing? A fintech relying on digital marketing, analytics or customer engagement tools?

If you assume that data used by financial services entities is subject only to federal and not Connecticut state privacy law, that assumption may no longer be valid under Connecticut's data privacy amendments. As a result, your compliance obligations may require a fresh look.

Effective July 1, 2026, amendments to the Connecticut Data Privacy Act narrow the safe harbor for data used by banks, insurance companies and other financial services companies regulated under the federal banking statute, the Gramm-Leach-Bliley Act.

The CTDPA also modifies applicability thresholds and definitions of covered entities. These changes affect not only traditional financial institutions, but also fintechs, payment processors, marketplace lenders, tax preparers, debt collectors, auto dealers and other businesses handling consumer data. In particular, companies using data at the intersection of finance, marketing and analytics may be affected.

The Connecticut Attorney General's Office, which is responsible for enforcing the Connecticut privacy laws, is watching.

In the annual enforcement report released in February, Connecticut Attorney General William Tong emphasized that businesses should expect that the Connecticut Attorney General's Office's enforcement agenda will track the recent amendments. In particular, it plans to focus on how businesses handle sensitive data and honor the data rights of Connecticut residents.

From Blanket Exemption to Data-Level Carveout

The CTDPA amendments narrow the exemption from any "financial institution or data subject to" the GLBA to only "data subject to" the GLBA.

The question will no longer be as simple as whether a company is subject to the GLBA, but now will require analysis at the data level. For example, marketing analytics conducted by a financial services entity previously covered by the entity-level exemption now may require analysis of specific data usage and compliance obligations under the CTDPA.

Instead of the broad GLBA entity-level exemption, the amendments substitute targeted exemptions for banks, credit unions, or their affiliates and subsidiaries directly engaged in financial activities regulated by the Connecticut Department of Banking or a federal bank regulator. A separate exemption applies to the activities of agents, broker-dealers, investment advisers and investment adviser agents regulated by the Connecticut



William Roberts



Laura Himmelstein



Jacob Buttiker

Department of Banking or the U.S. Securities and Exchange Commission.

These carveouts are narrower and more focused on specific activities than the former GLBA exemption and, significantly, do not automatically extend across all affiliates, subsidiaries or lines of business.

Lower or No Minimal Thresholds for Businesses Processing or Selling Personal Data

Under the law in effect before July 1, the CTDPA generally applies to entities that conduct business in Connecticut or target Connecticut residents and process personal data of at least 100,000 persons annually or, for entities with more than 25% of revenues from personal data sales, only 25,000 persons.

The amendments will eliminate the revenue-based trigger and lower the threshold from 100,000 to 35,000 persons, with no threshold at all for sensitive data — although payment transaction data is excluded. These changes shift the focus from the volume of data to the nature of the data processing.

More Companies and Business Lines Need To Pay Attention

Beyond traditional financial services, other consumer-facing businesses that handle consumer data — like auto dealers, retailers, loyalty programs, and ad tech and analytics firms — may now be regulated in ways that they did not experience before these amendments.

Marketing and ad tech activities, such as lead generation and data enrichment, also now may be covered by the CTDPA. Fintechs and other hybrid businesses whose models blend regulated financial activity with digital advertising, lead generation, analytics, embedded finance or cross-selling may be especially affected by these changes.

Even if data processed for certain purposes, such as banking or payment transactions, remains exempt, data processed for other purposes — such as marketing, website optimization or customer engagement — may now be regulated under the CTDPA.

Additional Compliance Obligations for More Companies

Organizations newly brought within the statutory scope need to establish new processes to comply with the CTDPA. These include processes and electronic systems to address consumer rights, including rights to access, correct and delete personal data; obtain a portable copy; and opt out of targeted advertising, sale and certain profiling.

In addition, consumers' expanded rights to opt out of sales of data and profiling, including any processing involving automated decision-making, may require updates to data management systems and marketing programs.

Third-party suppliers also are affected, given that consumer rights apply wherever the data is stored. Organizations will need to cascade their obligations — and ability to respond to consumer requests — throughout their supply chain to vendors, contractors and other downstream recipients of consumer data.

Third parties purchasing personal data also may be in scope for consumer requests demanding lists of all data recipients. Notably, different datasets even in the same system

may be treated differently, with some data exempt and other data covered by the CTDPA.

Next Steps for Compliance and Risk Mitigation

To prepare to comply by the effective July 2026 date, organizations are advised to identify previously exempt datasets that now will be covered by the state privacy law. That data mapping will enable organizations to pinpoint required updates to privacy notices, cookies disclosures, consumer rights processes, vendor agreements, and internal and external data governance.

Companies also should evaluate whether marketing, analytics and cross-selling activities trigger new obligations. These compliance steps are required to address consumer rights consistently across all systems where in-scope personal data resides.

As just one example, analytics using customer financing information to market insurance products may now be covered. Furthermore, the amendments may now cover entirely different industries, such as fintechs and auto dealers, which were not previously in scope for the CTDPA. Now, those datasets and industries will be subject to the CTDPA and enforcement activities announced by the Connecticut Attorney General's Office.

Proactive steps taken now will help companies satisfy regulatory expectations and manage risk while also strengthening customer trust.

William Roberts is a partner and leader of the data protection, privacy and cybersecurity practice, Laura Land Himmelstein is counsel and Jacob Buttiker is an associate at Day Pitney LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.