CLIENT ALERTS & INSIGHTS

Connecticut Joins the Fray; Enacts Data Protection Law That Mirrors Other Recent State Data Protection Laws

MAY 23, 2022

Beginning next summer, business that meet certain thresholds must comply with the Connecticut law, including several—now common place—individual privacy rights and a requirement to obtain opt-in consent before processing sensitive data.

In early May, Connecticut joined a number of other states in the last couple of years that have implemented data protection laws, in passing its own data protection law called the "Act Concerning Personal Data Privacy and Online Monitoring" (the "**Connecticut Law**").

The Connecticut Law takes effect on July 1, 2023, giving in-scope business a little over a year to prepare for the law's requirements. Utah became the first state in 2022 to enact its own data protection law when it passed the Utah Consumer Privacy Act in March. Previously in 2021, Colorado and Virginia passed their own versions of a data protection law, with both taking effect on January 1, 2023.

California, which was the first US state to enact a data protection law, also amended the existing California Consumer Privacy Act ("**CCPA**") in 2020 when voters passed the California Privacy Rights Act ("**CPRA**") via referendum. The CPRA will also take effect on January 1, 2023. The flurry of state activity in the data privacy and data security space is expected to continue, and possibly pickup, as Congress failed to take up an omnibus data protection law at the federal level.

For a comprehensive look at the state laws that are closest to effect and their respective requirements, see Data Meets World's state-by-state breakdown.

Generally, the Connecticut Law follows in the footsteps of recent US state laws and the European Union's General Data Protection Regulation ("**GDPR**"). Many of the law's requirements will be familiar to businesses that have dealt with the GDPR. Specifically, the Connecticut Law sets up a controller - processor dynamic and data protection principles (e.g., transparency, minimization, etc.)

Scope and Applicability

The Connecticut Law will apply to any business that operates in or commercially targets Connecticut residents and that meets one of the following thresholds in the preceding 12 months: (1) controls or processes the personal data of 100,000 or more Connecticut consumers; or (2) controls or processes the personal data of 25,000 or more Connecticut consumers while also deriving more than 25% of its annual gross revenue from selling personal data.

It is also important to note that the Connecticut Law specifically excludes personal data collected and processed solely for payment transactions. Any personal data connected to such transactions (so long as it is only used for the purpose of the transaction) does **not** count towards meeting one of the two thresholds.

The thresholds set forth in the Connecticut Law track very closely with those set forth in Virginia and Utah; however in both of those states, the second threshold require 50% or more of the business's annual gross revenue to come from selling personal data. Meaning, the businesses could more easily fall within the scope of the Connecticut Law.

Under the Connecticut Law, some categories of personal data that are already regulated at the federal level (e.g., protected health information under HIPAA; personal information under Gramm-Leach-Bliley Act; etc.) are excluded from the law's requirements. Further, the Connecticut Law does not apply to non-profit entities or to personal data collected in the employee-employer context; which aligns with Colorado, Virginia, and Utah. Therefore, unlike in California (where the employee-employer exemptions expire at the end of the year), employee personal data is excluded.

Personal Data and Sensitive Data

The Connecticut Law sets forth two categories of regulated data: (1) personal data; and (2) sensitive data.

Personal data is broadly defined (as it is in other data protection laws) to include any information that is, or reasonably could be, linked to an identified or identifiable individual.

Sensitive data is set up under the Connecticut Law as a subset of personal data. Under the Connecticut Law, sensitive data includes personal data related to (1) race or ethnic origin; (2) religion; (3) mental or physical health condition or diagnosis; (4) sex or sexual orientation; (5) citizenship or immigration status; (6) biometric or genetic data processed for the purpose of uniquely identifying someone; (7) precise geolocation data; and (8) personal data collected from a child.

Before processing sensitive data about an individual, a business must obtain that individual's prior opt-in consent under the Connecticut Law. This sensitive data opt-in requirement is also found in Colorado and Virginia's law.

Notice Requirements

A common thread in most data protection laws is a requirement that a business properly disclose its data collection and processing practices through a privacy notice.

Under the Connecticut Law, a privacy notice must include the following: (1) the categories of personal data processed by the business; (2) the purpose(s) for processing the personal data; (3) how an individual can exercise their applicable rights (explained further below); (4) the categories of personal data shared with third parties; (5) the categories of third parties personal data is shared with; and (6) an email address or other online contact tools for the individual to contact the controller.

If a business is selling data to third parties or processing personal data for targeting advertising, business must also "clearly and conspicuously" disclose in the privacy notice such activities and how an individual can opt-out.

Individual Rights

Individual data privacy rights have become a common underpinning in data protection laws, both internationally and in the US. The Connecticut Law aligns with this principle in providing individuals

with rights aimed at increasing an individual's access to and control over their personal data a business collects about them.

Under the Connecticut Law, individuals have the right (1) to access the personal data a business holds about them (except where such access would require the business to reveal a trade secret; (2) correct any inaccurate personal data; (3) to delete any personal data; and (4) to data portability (i.e., obtain a copy of their personal data in a readily usable format to the extent technically feasible and that such copy does not require the business to reveal a trade secret).

Further, similar to the data protection laws in Virginia and Colorado, individuals have the right to opt-out of (1) targeted advertising; (2) the sale of their personal data; and (3) any profiling in furtherance of automated decisions that produce legal or similarly significant effects.

"Targeted advertising" includes any advertising that is created and provided using the personal data obtained or inferred from that individual's activities over time and across websites or applications that are not affiliated with the business. A similar concept is found in the CPRA and is defined as "cross-contextual behavioral advertising." Targeted advertising does not include advertising that is based on the individual's activities on websites that are affiliated with the business.

In line with other data protection laws, "sale" is defined broadly to include any exchange of personal data for monetary or other valuable consideration. Sale does not include the transfer of personal data from a business (as a controller) to a third party acting as the processor (as further explained below).

Under the Connecticut Law and the third opt-out right listed above, "profiling" includes any automated processing that is performed to evaluate, analyze, or predict aspects related to an individual's economic situation, health, preferences, interests, reliability, behavior, location, or movements.

Controller - Processor Relationship

The Connecticut Law implements the common controller - processor relationship that businesses have become familiar under a number of US state laws and that has become the de-facto international standard under the GDPR. This contrasts with California, which establishes a business - service provider relationship.

In line with similar laws, Connecticut defines a "controller" as any entity that (alone or jointly) determines the purpose and means of processing personal data. Subsequently, "processor" includes any entity that processes personal data on behalf of a controller.

To effectuate a proper controller - processor relationship, the controller and processor must enter into a binding contract that delineates the parties' respective responsibilities and the processing instructions the processor must adhere to. The contract between the two parties must contemplate and provide that (1) each person involved in processing is subject to a duty of confidentiality with respect to the personal data; (2) at the controllers direction and option, for the processor to delete or return personal data to the controller (unless prohibited by applicable law); (3) audit and review obligations that allow the controller to ensure the processor is complying with the Connecticut Law; and (4) only engage subcontractors pursuant to written contracts that set forth the same or heightened obligations on the subcontractor.

Enforcement and Penalties

There is no private right of action under the Connecticut Law that would allow individuals to sue businesses. The Connecticut Attorney General is the lead enforcer. Businesses that violate the Connecticut Law can face civil penalties of up to $5,000 per willful violation.

Between July 1, 2023, and December 31, 2024, businesses will have an opportunity to cure any alleged violation after the Connecticut Attorney General provides notice to the business. The business will then have 60 days to cure the violation. This cure period will sunset in 2025 meaning beginning January 1, 2025, businesses will not have an opportunity to cure a violation before penalties are imposed.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.