GOODWIN

ALERT · JUNE 24, 2025

New York's Child Data Protection Act Is Now In Effect: What You Need to Do

BY Omer Tene Reema Moussa

On June 20, 2025, the New York Child Data Protection Act (CDPA) took effect, ushering in some of the most comprehensive child and teen privacy protections in the United States. The law applies to operators of websites, apps, connected devices, and other online services accessible in New York and covers the collection and processing of personal data from users under 18. Unlike the Children's Online Privacy Protection Act (COPPA), which protects only kids under 13, the CDPA extends its protection to users under 18, dramatically reshaping how online services interact with younger users. Shortly before the CDPA's effective date, New York's Office of the Attorney General (OAG) issued guidance regarding the law's definitions, requirements, and implementation.

Coincidentally, the same week, the Federal Trade Commission's (FTC) new COPPA rules update enters into effect June 23, 2025. And the Senate Commerce Committee will convene an executive session on June 25, 2025, to consider Sen. Ed Markey's Children and Teens' Online Privacy Protection Act (S. 836).

Over the past few years, with the effects of mobile phones and social media becoming a lightning rod for political debate, child privacy and online safety laws have been areas of particular focus — drawing bipartisan action across state and federal systems alike. Between the FTC's new COPPA rule updates, the Take It Down Act being signed into law, and several states passing age-appropriate design codes, even at a time of key regulatory downshifts, child privacy is not slowing down. New York is leading the way in this respect, with two new child protection laws: the CDPA and the Stop Addictive Feeds Exploitation (SAFE) for Kids Act, which is focused on mitigating kids' and teens' screen addiction.

Who Is Covered

The CDPA applies to operators who collect, maintain, or allow the collection of personal data from users in New York who are under 18 — because either the service is directed primarily to minors or the operator has actual knowledge of a user's age. The statute captures a broad swath of digital services and explicitly includes cases in which third parties are permitted to collect data through integrations or disclosures by users themselves.

Operators are also required to treat a user as a covered minor if the user's device or browser sends a signal — such as a privacy setting or plug-in — indicating that the user is (or should be treated as) a minor. This "age signaling" or "age flag" requirement is likely to spur new technical compliance innovations and challenges for platforms and publishers. Even on a general audience site, once an operator views an age flag, they must treat the user as under 18.

Data Processing Is Restricted

The law distinguishes between two groups of minors:

- For **users under 13**, operators can only process personal data if done in compliance with COPPA.
- For **users aged 13 to 17**, operators may not process personal data except if a teenager expressly opts in or the processing is strictly necessary for one of the specific purposes enumerated by the law. These purposes include
  - providing or maintaining a product or service requested by the user;
  - conducting internal business operations —*excluding* marketing, advertising, R&D, providing products or services to third parties, or prompting use of the service when not in use;
  - fixing technical issues;
  - preventing malicious, fraudulent, or illegal activity;
  - complying with legal obligations or government inquiries;
  - handling legal claims;
  - responding to security threats; or
  - protecting an individual's vital interests.

A prompt for teenager consent must be presented clearly and separately from other content, offer a meaningful choice (i.e., an equally prominent option to refuse data processing), and be freely revocable. It must not be requested more than once annually, and it cannot involve dark patterns. Operators may not condition access to the service on providing consent. Additionally, any consent signals from device browsers or plug-ins (such as global privacy controls) must be honored.

Notably, the New York OAG guidance notes that a business may not circumvent the "strictly necessary" requirement "simply by marketing its core service as one that includes tracking a covered user's personal data to support personalization such as behavioral advertising or creating a profile on a specific individual to display or prioritize certain media." This will have significant implications for companies that leverage personalization, content ranking, or otherwise behavioral or inferential profiling as a function of their business, since all these activities will now require express consent.

Selling and Sharing Are Restricted

The CDPA flatly prohibits the sale of minors' personal data and requires operators to have robust contracts, essentially data privacy addenda (DPAs), with all third parties and service providers. These DPAs must comply with detailed requirements, including notice obligations when third parties process covered user data on the operator's platform or the service is directed to minors. Operators must also identify minors' data to downstream recipients — a provision that may require updates to data classification and tagging systems.

Ad Tech and Behavioral Profiling Under Pressure

The CDPA will significantly impact digital advertising models involving minors, including teenagers, a cohort with significant purchasing power and a long horizon as consumers. Personalized ad targeting, behavioral profiling, or engagement-driven content feeds will require opt-in consent from teens — and are generally off-limits to users under 13 unless COPPA-compliant. Real-time bidding, audience modeling, and third-party cookies are in tension with the law's restrictions.

Operators should evaluate how their ad tech stack interacts with users under 18, particularly on services that could be construed as "directed to minors." This includes reviewing vendor scripts, software development kits, and data flows to ensure they don't inadvertently trigger compliance obligations or violate the outright ban on data sales.

Deletion and Retention Rules

Once an operator becomes aware that a user is a minor, they must delete the minor's personal data within 14 days — unless processing is allowed under consumer protection laws, defined as strictly necessary under the CDPA, or conducted with informed consent. This is a notably short window that may force updates to internal workflows and raise new operational risks if age is determined retrospectively. The CDPA also implicitly pressures companies to revisit their data retention schedules and apply stricter default retention periods for youth data.

What to Do Now

To implement the CDPA, businesses should:

- **Audit** whether their website, product, or service (or any component of it) is directed to minors or used by known minors in New York state
- **Review age-gating, detection, and browser signal handling**, particularly in light of the law's device-flag requirements for age-signaling and consent
- **Update consent flows** to meet the CDPA's informed consent standards, especially for teen users
- **Map and classify youth data** so it can be properly flagged for deletion or restricted processing
- **Review all vendor contracts** and flow down CDPA obligations where third parties may access or process minors' personal data
- **Assess ad tech deployments**, including embedded third-party tools, cookies, and profiling systems, and consider implementing opt-in functionality for non–strictly necessary functions if applicable

Age-Appropriate Design Codes and the SAFE for Kids Act

In addition to the CDPA, New York passed the SAFE for Kids Act in June 2024, an age-appropriate design code–style law that prohibits social media platforms from using addictive algorithms for users under 18. The law also requires platforms to implement age verification methods, granting the New York attorney general rulemaking and enforcement authority regarding the act. Similarly to age-appropriate design codes in other states (such as California and Maryland), the law may face legal challenges, with civil society and other stakeholders expressing concerns about potential violations of constitutional rights and the practical implications of implementing such laws.

Final Thoughts

The New York CDPA is more than a local extension of COPPA — it's a sweeping framework that expands privacy protections from children to teens and places their privacy at the center of digital product design and operation. With its broad definitions, strict limitations on advertising and data sharing, and short turnaround for compliance, the law sets a new benchmark in US child privacy regulation, and it is the first act in a wave of kids' and teens' privacy legislation to cross the finish line.

We would like to thank Federica De Santis for their assistance with this alert.

CONTACTS

GOODWIN

Omer Tene
Partner

otene@goodwinlaw.com
Boston | +1 617 570 1094

Reema Moussa
Associate

rmoussa@goodwinlaw.com
New York | +1 917 229 7870