ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
OCTOBER 22, 2025

# New York Child Data Protection Act: Additional compliance for businesses with online platforms

ANNA CLARK AND MARIA TEVES

**VIEWPOINT**
Maria Teves and Anna Clark

For years, the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501-6506), a federal law, has protected the personal information of children under 13. The New York Child Data Protection Act (CDPA) (N.Y. Gen. Bus. Law § 899-ee et. seq.), effective as of July 1, 2025, imposes similar requirements that apply to a broader swath of minors, or those under the age of 18.

The CDPA applies to companies that operate a website, online service, application or connected device (for ease of reference, henceforth referred to as "platform") that is used by or targeted to minors under the age of 18 within New York State, and may apply to third parties as well, when processing minors' personal information. The CDPA requires pre-processing consent, restricts data processing for advertising and profiling, bans retaliation against those who withhold consent, prohibits the sale of personal information, imposes additional obligations on the disposal of minors' personal information and notice of change in data protection status when the minor becomes an adult. Violations carry penalties of $5,000 per minor impacted, and per violation.

## WHO MUST COMPLY WITH THE CDPA

The CDPA applies to a person or entity (Operator) that operates a platform and who controls the purposes and means of processing personal data, to the extent that such platform is used by or "primarily directed to minors."

A platform is "primarily directed to minors" if: (1) it directly targets minors as users or (2) it knowingly collects personal information from users of other websites or services primarily directed to minors. Simply providing tools or links to child-focused sites does not qualify as being a platform primarily directed to minors.

The CDPA also applies to Processors (those who handle personal information on behalf of, and subject to the Operator's instructions) or Third-Party Operators (those who collect or use data for their own purpose as agreed upon with the Operator). Disclosure of minors' personal information to these Processors and Third-Party Operators must be subject to a written agreement that meets certain requirements, including, among others, specification of the nature and purpose of the data processing, permitted use(s) of data, and the rights and duties of the parties. Further, the Operator must disclose to these third parties, before collection or processing, whether the platform is directed to minors or when the data concerns a minor under 18. Note that Third-Party Operators may be excused from complying with certain requirements if they are reasonably informed that the Operator obtained consent, or if they lack actual knowledge that the relevant user is a minor and that the Operator's platform is primarily directed to minors.

## SUMMARY OF SOME NOTEWORTHY REQUIREMENTS

The CDPA protects the personal data of "covered users" in New York who are actually known to be minors (under 18) or users of platforms that are primarily directed to minors even if the Operator has no confirmation of the exact age of those users. Personal data is "any data that identifies or could reasonably be linked, directly or indirectly, with a specific natural person or device."

A minor's personal data may only be processed upon verifiable parental consent for minors under 13. The CDPA maintains the same consent protections of minors and allows

teens aged 13-17 to give informed consent before their personal information is processed.

The COPPA and CDPA share a common objective to safeguard minors from misuse of their personal information online; however, their scope and protection mechanisms differ. The distinctions below are particularly significant for Operators that may be subject to overlapping federal and state obligations:

- **Age and territorial coverage.** COPPA protects children 12 and under in the U.S., while the CDPA protects all minors under 18 within the State of New York.
- **COPPA** is a federal law and requires the compliance of all U.S.-based operators and those who have platforms directed to U.S. children. The CDPA applies to any Operator (or Processors and Third-Party Operators), regardless of location, whose platform is primarily directed to or used by minors under 18 within New York.
- **Exceptions to consent.** There is no exception to the requirement of verifiable parental consent for children under 13, whether under COPPA or CDPA. Under the CDPA, informed consent may not be required when the processing of personal data of teens aged 13-17 is for the following permissible purposes: providing a requested service, protecting someone from fraud or similar acts, managing security risks or legal claims, or complying with legal or regulatory obligations. Notably, under the CDPA, a minor's user's personal data may not be processed for marketing, advertising, research or profiling purposes or for prompting inactive users, except that it may be allowed for teens aged 13-17, subject to informed consent.

In addition to the requirements above, there are key restrictions and obligations under the CDPA:

- **Specific and standalone transaction for informed consent.**
  - The request for informed consent must: be separate from any other transaction, not pressure a user into consenting, clearly state that processing is not required, notify that the minor will not be blocked from continued use of the platform for refusal to consent, and display the refusal to consent option as the most prominent option.
- **No retaliation for refusal to consent.**
  - Operators may not restrict, reduce the quality, or increase prices of products and services when they do not obtain verifiable parental consent under COPPA or the CDPA.
- **Prohibited sale of minors' data.**
  - Operators may not purchase or sell or allow Processors or Third-Party Operators to purchase or sell the personal data of a minor.
- **Timely data disposal.**
  - Within 30 days after determining or being told that a user is a minor, the Operator, Processor, or Third-Party Operator must delete the minor's personal data unless COPPA allows or when strict necessity applies, or informed consent is obtained under the CDPA.
- **Aging-out notices.**
  - When an entity learns a user is no longer a minor, it must pause processing the user's personal information and give notice that the rights and protections under the CDPA may no longer apply to the user.

## POTENTIAL CONSEQUENCES FOR NON-COMPLIANCE

Non-compliant organizations may be ordered by the Attorney General to stop offending business practices or to delete data, return profits or gains in addition to imposing fines of up to $5,000 per minor impacted per violation, along with other appropriate penalties. While the law does not explicitly authorize private causes of action, individuals may pursue lawsuits that cite the CDPA as an industry standard to claim that they are entitled to damages resulting from violations of the law. Businesses can also suffer from negative publicity, diminish consumer trust, or face disruption of operations (if they become subject to a government investigation or lawsuits).

Accordingly, it is important for companies to review their compliance procedures, especially in conjunction with data privacy obligations under other applicable state and federal laws and seek guidance from experienced professionals regarding the ever-evolving technological and legal landscape, including the CDPA.

*Anna Mercado Clark, Partner and Chief Information Security Officer at Phillips Lytle, as well as Co-Leader of the firm's Technology Industry Team, can be reached at aclark@phillipslytle.com or 212-508-0466.*

*Maria Althea M. Teves, attorney at Phillips Lytle, focuses her practice on cybersecurity and commercial litigation. She can be reached at mteves@phillipslytle.com or 716-847-5415.*