SK&C SIGMAN, KHAN & CHUBB, PLLC

Update Regarding the Children's Online Privacy Protection Rule (COPPA)

Effective April 22, 2026

75 State Street, Ste. 100
Boston, MA 02109
Phone: 617-758-8212
www.skclegal.com

Amendment Notification Regarding The Children's Online Privacy Protection Rule

The Children's Online Privacy Protection Act ("COPPA") was enacted by the federal legislature in 1998 to help protect the privacy of young children's information, and the Children's Online Privacy Protection Rule ("COPPA Rule," "Rule") is a federal regulation issued by the Federal Trade Commission under the law to implement and enforce enhanced protections for children's personally identifiable information. The Rule prohibits, "the unfair or deceptive acts or practices in connection with the collection, use and/or disclosure of personal information from and about children on the internet."

Our clients who provide commercial websites or online services that are directed to children under age 13 or who knowingly collect, use, or disclose personal information from children in this age group are subject to the Rule and defined as "operators." As an operator, we want to inform you of recent amendments to the Rule that reflect a response to the evolving landscape of data collection online and a continued mission to protect the privacy and safety of minors using online services. The amendments to the Rule as explained below strengthen security procedures regarding children's personal information along with notice and consent requirements for parents, allowing for more parental control over how and where their child's personal information is shared.

These amendments will come into effect on April 22, 2026, and require mandatory compliance for operators subject to the COPPA Rule.

Expansion of Definition of Personal Information: In addition to direct identifiers such as names and email addresses and persistent identifiers such as IP addresses, device identifiers or customer numbers held in a cookies, geolocation information, photos, videos, and audio containing a child's voice or image that are considered "personal information" under the Rule, the definition of "personal information" has been expanded to include biometric identifiers such as fingerprints, handprints, retina patterns, iris patterns, genetic data, including a DNA sequence, voiceprints, gait patterns, facial templates, or faceprints. "Personal information" shall also include government-issued identifiers such as a social security number, a birth certificate, a state identification card, or a passport number.

Clarification of Definition of a Mixed Audience Website: A "mixed audience website" has been clarified under the rule to be defined as a site or service directed toward children under the criteria of the Rule, but which does not target children as its primary audience. This is significant because operators of mixed audience websites must implement neutral age screening mechanisms from all users before collecting personal information. If a user is identified as 13 or older, the operator may collect personal information without obtaining parental consent under the Rule. However, if a user is identified as under 13, data collection must stop until verifiable parental consent is obtained.

Operators of mixed audience websites may collect limited personal information before age screening only for specific internal operations and safety purposes such as providing parental notice, responding to a one-time request from a child, or protecting a child's safety.

Limited Exception for Need of Verifiable Parental Consent for Audio Files. Under the amendments, the Rule makes clear that although audio files of a child's voice are considered personal information, operators may collect a child's voice (as long as it does not provide additional personal information such as the child's name) without first getting verifiable parental consent in the limited situation where all of the following are true: 1) the audio was captured solely to respond to the child's request; 2) the personal information is only used to respond to the request, 3) the operator does not disclose the personal information; and 4) the operator deletes the audio recording immediately after responding to the request.

Expansion of Methods of Obtaining Verifiable Parental Consent: Under the COPPA Rule, verifiable parental consent is required before an operator, collects, uses or disclosures personal information from a child under 13 unless an exception applies as mentioned above. In addition to long-established methods of obtaining verifiable parental consent under the Rule such as a signed physical or electronic consent form, requiring a payment instrument that provides notice to a parental account holder, providing a toll-free number or video call to confirm identity, knowledge based questions that children would not know the answer to, and providing government-issued ID verification which the operator verifies and then deletes, the Rule has been expanded to include gathering consent through the use of a mobile phone number.

The Text-plus method of obtaining verifiable consent involves using text messages to the provided mobile phone number. The consent obtained via text message should be confirmed via a follow-up text message to the parent following receipt of consent, or by sending a letter or making a telephone call to the parent at an address or telephone number provided. An operator that uses this method must also inform parents that they can revoke their consent given in response to the earlier text message at any time.

Verifiable Parental Consent Required for Non-Integral Sharing of Personal Information: The amendments to the Rule now require separate verifiable parental consent if an operator intends to disclose a child's personal information for purposes that are non-integral to the services such as advertising, monetary disclosures, or disclosures used for the training or development of Artificial Intelligence ("AI"), including but not limited to third-party cloud AI Application Programing Interfaces, shared training datasets or third party analytics. If an operator collects a child's personal information in any form such as raw data, embeddings, biometric templates or model-generated identifiers, this is still considered use and collection for which verifiable parental consent would be required.

Expansion of Direct Notice (Targeted Consent Request) Requirement: Before verifiable parental consent is provided for the collection of personal information, direct notice must be made to the parent of the child whose information is sought.

Under the amendments, the content of the direct notice, which is sent directly to a parent, is required to be more detailed and specific to assist parents to decide whether to provide verifiable parental consent. The direct notice must tell parents that the operator wishes to collect personal information, what specifically will be collected as personal information, and how the operator intends to use the personal information collected from a child. It must inform parents that parental consent is required and how to provide it as well as their right to review personal information collected, request its deletion, or revoke consent.

Also, as per the amendments, if personal information will be disclosed to third parties, operators must include the identities and categories of third parties, the purpose of the disclosure, and whether any personal information will be made public.

The direct notice must also include information informing parents that third party sharing is optional, specifically the notice must inform parents that they can agree to let the website collect and use their child's personal information without consenting to disclose the personal information to third parties unless the disclosure is integral or necessary for the website or service to work properly to provide the requested services. Non-Integral disclosures require separate verifiable parental consent as discussed above. Operators are specifically prohibited from conditioning service access on consent to non-integral disclosures under the Rule.

The direct notice shall also inform parents that if they do not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's or child's online contact information and the parent's or child's name from its records.

Changes to Notice Given on Website or Online Services: Operators must post clear, prominent links to comprehensive online notices detailing their privacy practices regarding children's information. Under the Rule changes, the notice must now provide information regarding the operator's data retention policies detailing how long children's personal information will be stored.

The online notice must now also disclose the identity and category of all third party recipients of children's personal information along with the purpose of the disclosure.

Information Regarding Internal Operations: The operator must provide information regarding how internal operations on the site or online service are using persistent identifiers and the means employed by the operator to ensure that the use of the persistent identifiers is only used as specifically permitted to provide support for the internal operations of the website or online services, not for other unapproved purposes such as tracking or contacting specific individuals for behavioral advertising.

Enhanced Security Program: Operators must design, implement and maintain a written information security program with necessary safeguards tailored to the amount and sensitivity of the information collected from children and risk of harm from unauthorized access or misuse

including conducting risk assessment, monitoring, and testing of safeguards at least as often as once a year.

An employee or several employees shall be appointed to manage and coordinate the operator's written information security program. The operator must assess, review, and update the written information security program annually to reflect technological improvements or other changes that may affect the program's effectiveness.

- A major change as outlined in the amendments is that operators must now ensure that third party's access is limited to only what is necessary and that any third party with access to children's personal information also maintains appropriate safeguards. This includes conducting due diligence before sharing personal information with third parties as well as ongoing monitoring to ensure third party compliance. Operators must actively review, verify, and document third party security policies and practices and obtain written assurance that these third parties are properly securing children's personal information in alignment with the Rule's requirements including not using the information for unauthorized purposes.

Limits on Data Retention: Operators covered by the Rule must limit the retention of children's personal information to only as long as reasonably necessary to fulfill the original purpose for which the children's information was collected. Indefinite storage of children's information is not allowed under the Rule. Once data is no longer needed, it must be deleted securely to prevent unauthorized access or use.
Operators must provide public disclosure of the written date retention policy and must include the privacy notice on the website or online notice clearly explaining why data is collected, what data is needed, and a clear timeframe for its deletions.

New Transparency Requirements for Safe Harbor Programs: Safe Harbor Programs allow industry groups to set self-regulatory guidelines which have been approved by the Federal Trade Commission ("FTC") that offer the same or greater protections than the COPPA Rule. The purpose is to help companies ensure compliance, reduce legal risks and avoid formal FTC enforcement actions.

Under the new amendments, approved Safe Harbor Programs must provide more information to the FTC and the public. Safe Harbor Programs must conduct: 1) due diligence to determine the security and data practices of participating operators; 2) publicly list on their website or online services the identities of operators participating in the program as well as those who have left; 3) include the specific certified website, operating system or online service for each operator; and 4) provide in the annual report a description of each disciplinary action against an operator as well as the description of the process used to determine whether an operator used to determine whether an operator required discipline.

Key Take Aways

The amendments to the Rule significantly expand the obligations and responsibilities for operators requiring increased transparency by outlining new notification requirements as well as new requirements regarding gathering verifiable parental consent as well as additional obligations regarding safeguarding the security of personal information including strengthening operator accountability for the collection and use of private information by third party vendors or partners.

Recommendations

- Visit https://www.ftc.gov/legal-library/browse/rules/children-online-privacy-protection-rule-coppa to familiarize yourself with the Rule including the amendments.
- Determine whether you are an operator under the definition of the Rule.
- Determine whether your site or online service is a mixed audience site as defined by the Rule requiring mandatory age screening mechanisms.

If you are an operator, you should:

- Review all information that is collected from children under 13 to determine the types of personal information that is collected.
- Implement or update age screening mechanisms as necessary. Eliminate collection of personal information until notices and updated verifiable parental consent procedures are in place.
- Determine who the third parties are that are receiving personal information from you as well as the specific types of data that is shared to assess whether the data is integral or non-integral to providing your services.
- Gather contact information and contractual assurances from these third parties with whom you share personal information requiring their compliance with the COPPA Rule and set up practices of due diligence and continued monitoring.
- Revise direct notices to parents to ensure the required information is included as per the amendments.
- Ensure direct notices are sent and verifiable consent is obtained through reasonably designed methods in light of available technology to ensure that the person who is giving consent is the child's parent such as by using the examples of the acceptable methods for obtaining verifiable parental consent as outlined in the Rule before personal information is collected or shared.
- Update privacy policies, security procedures including a formal written information security program, and data retention policies as necessary to comply with the amendments.
- Participants in Safe Harbor Programs should review compliance with self-regulatory guidelines and provide information as necessary for the Safe Harbor Program's compliance with Rule obligations.

Conclusion

Assessing whether the Rule is applicable as well as navigating the requirements and exceptions to the Rule can be complex and mistakes could subject clients to potentially significant fines. Please contact our office to discuss a privacy compliance audit before April 22, 2026.
We can help by performing a legal review of your privacy procedures and updating your privacy policies and contracts with outside parties to ensure compliance with the amendments as necessary.

Although the COPPA Rule changes are directed toward businesses who collect information from children under 13, we urge all clients who provide online services or websites to review data collection practices and privacy policies for ongoing compliance with tightening state and federal regulations regarding safeguarding personally identifiable information regardless of age.

Updated March 24, 2026