Consent for the Collection, Use, and/or Disclosure of Children's Personal Information

A Comparative Analysis for EdTech of the U.S. and EU Frameworks

Emily G. Cramer, CIPP/US

iapp

The education technology industry (known as EdTech) is one of the leading growth areas for technology in the world; one estimate suggests "investments [are] set to reach $252 billion globally by 2020." EdTech uses technology to: teach technology, enhance the educational process, aid educators through efficiency and effectiveness, and promote education. The prolific use of EdTech in and out of the classroom has enabled educators to use data to look at historical trends as well as real-time data on lesson efficacy. This paper will address the particular differences between obtaining consent under the General Data Protection Regulation (GDPR) and the various U.S. frameworks for the EdTech industry.

The prolific use of EdTech in and out of the classroom has enabled educators to use data to look at historical trends as well as real-time data on lesson efficacy.

Part I: Children's privacy — U.S. framework

The Family Educational Rights and Privacy Act of 1974

In 1973, a year before the Family Educational Rights and Privacy Act was signed into law by President Ford, an advisory committee of the Department of Health, Education and Welfare published a report — which later became the basis of the Fair Information Practices as adopted in 1980 by the Organization for Economic Cooperation and Development — addressing the lack of privacy protections in the law and proposing fair information principles to address this issue. FERPA, which became effective Nov. 19, 1974, addressed specifically the privacy protections of student education records and applies to all schools that receive federal funds for education. Four months after its enactment, FERPA was amended in order to clarify the law. In a joint statement by Sens. James Buckley and Claiborne Pell, the sponsors of the amendment, it was stated that "the purpose of the Act is two-fold — to assure parents of students, and the students themselves if they are over the age of 18 or attending an Institution or postsecondary education, access to their education records and to protect such individuals' rights to privacy by limiting the transferability of their records without their consent." The amendment clarified the role of educational agencies and institutions was to "conform to the fair information record-keeping practices" as first proposed in the HEW Report.

Since its enactment, FERPA has been amended nine times, including the Protection of Pupil Rights Amendment, which requires prior parental notification and opportunity

for opt-out before the administration of student surveys, analyses, and evaluations that request a student to reveal:

- Political affiliations or beliefs of the student or the student's parent.
- Mental or psychological problems of the student or the student's family.
- Sex behavior or attitudes.
- Illegal, anti-social, self-incriminating, or demeaning behavior.
- Critical appraisals of other individuals with whom respondents have close family relationships.
- Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers.
- Religious practices, affiliations, or beliefs of the student or student's parent.
- Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

Additionally, PPRA requires covered educational agencies and institutions to provide notice at least annually of the rights of students under PPRA.

"Written consent" under FERPA:

Written consent under FERPA must be obtained prior to the release of any information from a student's education record (except where otherwise permitted) from the parent or the eligible student. A written consent must include notice to the parent or eligible student that "specif[ies the] records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents."

> *Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. The actual means of notification … is left to the discretion of each school.*

Because of the diversity of EdTech services used by educators, whether or not student information is protected by FERPA, and thus whether an EdTech company must comply with the written consent requirement requires an individual analysis to determine: (1) if FERPA-protected information is implicated; and (2) if so, has the educational agency or institution obtained consent or ensured that the contractual arrangement with the EdTech service meets one of the FERPA exceptions to the written consent requirement. However, FERPA may only protect the personally identifiable information of students through a covered entity — an educational agency or institution that receives funding from the U.S. Department of Education. Therefore, EdTech companies that provide services to individuals or organizations that do not fall within the regulated education system may need to consider how other U.S. laws, such as the Children's Online Privacy Protection Act, may require consent prior to processing personally identifiable information of children.

The Children's Online Privacy Protection Act

The Children's OnLine Privacy Protection Act makes it unlawful for a website or online service directed at children to knowingly collect personal information from a child without the parent's consent. Under COPPA, personal information is defined as any identifiable information collected online, such as: first and last name, whole or partial address, online contact information, screen name, telephone number, Social Security number, persistent identifier (such as IP address), photograph, video or audio file of the child's image or voice, geolocation information, or any information about the child or the parents of the child collected by the operator and combined with any other identifier. "The *primary goal* of COPPA is to place parents in control over what information is collected from their young children online … while accounting for the dynamic nature of the Internet." An operator of a website or online service directed at children (as defined under 16 C.F.R. § 312.2) must:

- Provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§312.4(b)).
- Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§312.5).
- Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§312.6).
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§312.7).
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§312.8).

A violation of COPPA is treated as a violation of the Federal Trade Commission Act as an unfair or deceptive act or practice.

Verifiable consent under COPPA

COPPA creates a different type of consent under the U.S. framework — it requires an operator to obtain "verifiable consent":

> *Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:*
>
> ***(1)** Receives notice of the operator's personal information collection, use, and disclosure practices; and*
>
> ***(2)** Authorizes any collection, use, and/or disclosure of the personal information.*

Similar to "written consent" under FERPA, operators must obtain verifiable consent prior to collecting personal information online from children under 13 years of age. However, verifiable consent "raises two distinct problems: first, how to authenticate the identity of the party that appears to be manifesting consent on behalf of a

student and, second, how to verify that party has appropriate authority within the school hierarchy to manifest consent." The FTC has noted that this authentication problem must be addressed through reasonable measures in light of the available technology, such as using a toll-free number, using a print and send method, or verifying a parent/guardian's identification against a database.

Operators providing online websites or services on behalf of educational institutions may not be required to obtain verifiable consent from a parent if a school is acting on behalf of the parent as an agent. "However, the school's ability to consent for the parent is limited to the educational context — where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose." In order for the operator to obtain verifiable consent from an agent, the operator must provide the same notices to the educational agency or institution as they would a parent and limit the data for educational purposes. The operator may also have to comply with FERPA and other state laws, such as California's Student Online Personal Information Protection Act, and have vendor contracts that safeguard privacy and security and prohibit secondary uses of that information.

The primary shortcomings of COPPA are that it only protects children to the age of 13, and only applies to operators who are knowingly targeting kids under the age of 13, "and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13."

The FTC "looks at a variety of factors to see if a site or service is directed to children under 13, including the subject matter of the site or service, visual and audio content, the use of animated characters or other child-oriented activities and incentives, the age of models, the presence of child celebrities or celebrities who appeal to kids, ads on the site or service that are directed to children, and other reliable evidence about the age of the actual or intended audience."

Part II: GDPR framework

Children's privacy under GDPR

Under the General Data Protection Regulation, "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. … In particular, [where] the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child." The GDPR also establishes that children are "vulnerable natural persons." Because of this, the GDPR says that "the risk to the rights and freedoms may result from personal data processing which could lead to physical, material or nonmaterial damage, in particular where personal data of vulnerable natural persons, … children, are processed." Therefore, the lawful processing of children's data is specifically addressed in Article 8 of the GDPR.

Article 8 of the GDPR only applies to "information society services" that offer services directly to a child under the age of 16, regardless of the lawful basis for processing under Article 6(1). Individual member states may lower the age, but not below 13 years old. Information society services is not defined by the GDPR, but it adopts by reference the definition in the

Directive 98/34/EC: "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." This broad definition includes ISPs, search engines and EdTech. It is worth noting that although Article 8 states that if a controller (and ISS) is using any legitimate purpose under Article 6 it must comply with Article 8, the U.K Information Commissioner's Office guidance on consent suggests that where possible a controller should rely on legitimate interests rather than consent.

Consent of the parent/ guardian under GDPR

Similar to COPPA, the GDPR requires a form of verifiable consent by the controller. Parental (or guardian) consent is required for all information society services that collect children's data, regardless of whether or not they have a lawful basis for processing. Unlike COPPA, however, the GDPR does not have a targeting requirement. Any offer of ISS directly to a child must obtain parental consent. However, it is the sole responsibility of the controller to make reasonable efforts to verify consent; assuming that the ISS does not "alone or jointly with others, determine the purposes and means of the processing of personal data" and that they are only a processor as defined in Article 4(8), the operator of an ISS would not be required to obtain verifiable consent under the GDPR. This means that an EdTech company that provides an ISS as a service for an educational institution may not be held responsible for obtaining consent under Article 8; the key issue is whether the ISS is a controller or a processor.

There are additional requirements for processing children's data under the GDPR. Because of the transparency principle under Recital 58 of the GDPR, any information and communication addressed to a child must be in clear and plain language. Where a parent has given consent for a child, consent may be withdrawn at any time. In addition, what complicates verifiable consent by a parent or guardian under the GDPR is that Article 8 permits member states to provide by law a lower age not below 13 years old for obtaining consent from the holder of parental responsibility, and validity, formation or effect of a contract in relation to a child. "Activities addressed specifically to children shall receive specific attention" by each supervisory authority in promoting public awareness about the risks, rules, safeguards and rights in relation to processing. This means that counter to providing a single framework under which all EU member states will function, the processing of children's data that is addressed to children will be one area in which EdTech will need to track each member state's laws to determine whether there are more strict requirements that will need to be followed.

Other than mandating that a controller must obtain verifiable consent, there is no specific method of consent under the GDPR as it relates to children. Therefore, a controller would need to comply with Article 7 of the GDPR. Consent, where used as a lawful method of processing, requires that: the controller can demonstrate that the data subject has consented, any written declarations made by the controller are presented in a manner clearly distinguishable from other matters, consent be given prior to processing data, it should be easy to withdraw consent, and consent must be freely given.

There are limited circumstances where parental consent is not necessary for children's data: where it is necessary to process children's data in the context of preventative counseling services offered

directly to a child, or where processing activities fall outside of the GDPR. Although there are no global rules, at least one commissioner has stated that parental consent expires when the child reaches the age of majority for the member state.

Part III: Key distinctions between the two frameworks

	FERPA	COPPA	GDPR
Type of Consent	Written	Verifiable	Verifiable, freely given
Applies to EdTech?	Only where organization receives Federal Funding from the DOE	Only where website is directed at a child	Only where EdTech is offering ISS to a child and is the controller
Permits educational institution to act on behalf of parent/guardian?	Yes	Yes	Controller – No Processor – In essence
Age of Majority	18 years old	13 years old	16 years old, but may be lowered by member states to no younger than 13 years old
Notice required	Notice of any disclosure of records to be released, the reasons for such release, and to whom, and with a copy of the records to be released	Notice of operator's collection, use and disclosure practices	Clearly distinguishable from other matters, and presented using clear and plain language easily understandable by a child
Withdrawal of consent permitted?	Yes	Yes	Yes
Right to erasure?	There is a process for disputed information, but ultimately it is up to the education institution to decide	Yes	Yes

While complying with the GDPR can be difficult, in reality the consent requirements under the GDPR for EdTech are very similar to the U.S. framework for children's privacy. A key distinction is that the U.S. framework clearly permits educational institutions to act as an agent (or on behalf) of parents and guardians, and transfers the responsibility of obtaining consent to the educational institutions themselves where EdTech is used by the institutions.

In contrast, where EdTech could be considered a joint-controller, it would be required under the GDPR to obtain verifiable consent. However, where EdTech clearly is acting as a processor on behalf of another entity (regardless of whether it is for an educational institution or not), it would not be required to obtain (or manage) consent. EdTech companies acting as controllers will be the most affected by the GDPR, as the management of verifiable consent, the time when that consent expires, and the additional requirements of transparency will be operationally significant. Where additional differences may arise in the near future is in the adoption of supplementary requirements related to children's privacy by the individual supervisory authorities and member states.