INTEROPERABILITY & GDPR

On May 25th, 2018, the General Data Protection Regulation (GDPR) went into effect. While GDPR only applies within the European Union (EU), the principles and requirements will have an impact in the United States as companies operating in the EU will have parts of their business governed by GDPR.

GDPR defines clear and sound privacy practices. Because data interoperability supports better data handling, there are multiple areas where data interoperability and the requirements of GDPR are mutually supportive.

DEFINITION OF PERSONAL DATA

The index of definitions used in GDPR begins with a definition for "personal data." The definition of personal data in GDPR goes beyond definitions of Personally Identifiable Information in FERPA. Because of this, it provides a clearer foundation to help vendors protect information that they collect.

DATA PROCESSOR AND DATA CONTROLLER

The notions of data processors and controllers aren't new to GDPR, but the clear split between the two is a useful frame that can help clarify conversations around data handling and potential privacy impacts.

Data controllers must be clear and transparent about how they collect and use information. Because interoperability standards clearly define data that can potentially be collected, the responsibilities of a data controller are easier to meet. Data controllers are required to understand "the nature, scope, context and purposes of processing" information. Because these elements are largely defined by interoperability standards, the obligations of data controllers are easier to meet.

Conversations about interoperability frequently run into concerns about how data is managed and handled by the organizations that collect it. Subcontractors that manage or handle data for the controller frequently get cited as problematic because the rules under which they manage data are not clear. Because interoperability unlocks information, the potential risk of unauthorized access or non-educational use increases. The larger and more accurate the data set, the more value within the data.

GDPR lists specific controls and actions that data controllers need to take to ensure that data processors handle data safely, and that data entrusted to processors are only used for specific purposes defined under a legally binding agreement between the processor and the controller.

The level of specificity required under GDPR is a great model for edtech companies. Many companies already go beyond what GDPR requires, and a subset of these companies describe how they work with data processors in their privacy policies.
CONSENT

Data interoperability standards provide clear definitions and rules around what data can potentially be collected. This clarity makes it easier to let people using the product know what information is collected and why. This transparency is an essential element of informed consent.

GDPR defines clear requirements about the conditions required to provide consent, and how consent must be freely given. The clarity and control provided by virtue of using an interoperability standard make it easier to create meaningful consent mechanisms that align with GDPR requirements.

DATA PORTABILITY

GDPR requires that companies provide users with copies of their data "in a structured, commonly used and machine-readable format." Because interoperability standards provide a blueprint for moving data in a secure and structured way, interoperability standards can help organizations meet this core requirement of GDPR.

DATA PROTECTION OFFICER

The benefits of implementing an interoperability standard are numerous, but with larger, more accurate, and more valuable data there is an increased security risk. As a result, companies that implement interoperability standards need to take proactive steps to demonstrate how they protect the information entrusted to them. Toward this end, the role of the Data Protection Officer -- which is sound practice for any organization managing significant amounts of information -- can help organizations create coherent and secure practices around handling information, and communicating about how they handle information.

GDPR also requires that companies implement privacy by design when it comes to protecting information entrusted to them. In this way, complying with GDPR can help companies develop or enhance both their existing privacy and security practice, and how they communicate about these practices.

SUMMARY

This document is a high level summary of some of the ways that data interoperability and the requirements of GDPR are mutually supportive. Each of these individual elements is significant on its own merits, but collectively, the benefits of using an interoperability standard makes it easier to comply with legal requirements like GDPR. The benefits of using an interoperability standard and the requirements of complying with GDPR both push organizations to be more intentional with how they use and protect the information required to provide their service.