Higher Education Working Group Meeting Notes

Friday, March 31, 2017
11:30am-12:30pm
Topic: E.U. General Data Protection Regulation (GDPR) and higher education
26 Attendees (see list of organizations at the end of the notes)

Amelia Vance (FPF)

- *State Legislation Update:*
  - 44 states have introduced 166 bills in 2017
  - 31 impact higher education (most – 135 – impact K-12). Trends and Interesting Legislation:
    - Bills expanding SLDS'
    - Bills restricting release of immigration status
    - Social media or log-in privacy bills (restricting institutions from requesting access to or the password for student social media and other online accounts)
    - Higher Ed SOPIPA legislation in Illinois (unlikely to pass this year)
- *Higher Ed and Student Privacy Laws Trends:*
  - 19 student privacy laws with implications for higher education have passed since 2013
    - Security breach and notification laws
    - Social media laws (see above)
    - Laws expanding SLDS'
    - A Maine law required the state superintendent to adopt FERPA-aligned rules
    - Law noting that any online writing or data created by a student belongs to the student
    - A Virginia law requiring that institutions keep mental health records confidential
    - A New Hampshire law banning PostSecondary and Workforce data in the SLDS and banning tracking of students who go to college outside of New Hampshire.
    - It is noteworthy that laws applicable to state education agencies may also be applicable to higher ed but are not included in the 19 laws.
  - FPF will be publishing a short report on these trends later this year.
- FPF is releasing our state legislative tracking spreadsheet to all FPF members later today. If you have not received it by April 4th, please contact Amelia at avance@fpf.org.
- **FPF has a GDPR Working Group now, and members are welcome to join. Please email Amelia at avance@fpf.org with any questions.**

Linnette Attai (PlayWell LLC)

Key Points:

- GDPR becomes effective in May 2018, replacing current E.U. data protection law with a broader and more uniform approach across the Member States.

- Fears surrounding GDPR arise from stiff penalties combined with the relative lack of implementation guidance from E.U. regulators.
- Most ed tech vendors will be classified under GDPR as "Data Processors" with respect to their school system clients, the "Data Controllers."
    - As Data Controllers, ed tech clients will be legally responsible for the activities of their Data Processors. This will lead to an increased focus on auditing, record-keeping, and due diligence requirements for Data Processors.
    - Ed tech companies must be able to provide guarantees to clients that you can meet GDPR requirements.

Brief Overview of GDPR

- Replaces current data protection law in the E.U. Member States.
- Responds to practical and political considerations that impacted uniformity and enforcement of current law. Allows more standardized application across Member States.
- Effective on May 25, 2018 with expectations that compliance be achieved by that date. Implementation will not be affected by Brexit—the U.K. will likely end up with a substantially similar law.

GDPR Core Principles

- Safeguards the individual's fundamental right of privacy. Prioritizes this individual right over that of a controller or processor to collect or use data.
- Requires a legitimate basis for processing data (e.g. a contract) and certain contractual protections for the data. Data processing can occur based on a legitimate interest of a data controller unless it would interfere with the rights of the data subject.
- Requires clear purpose specification. Processing practices must conform to the stated purpose.
- Enshrines data minimization, requiring entities to collect only the least amount of data necessary to provide the service.
- Requires data to be kept accurate or deleted. Also requires deletion upon conclusion of processing.
- Requires entities to take broad "appropriate measures" for security to protect against unlawful processing or data loss. These measures are judged against the "state of the art" relative to reasonable costs for the type of data stored.

GDPR Legal Framework

- <u>Broader reach than current law:</u> GDPR applies to anyone who offers goods or services to E.U. citizens or monitors the behavior of E.U. citizens, no matter where you are located.
- <u>Broader definition of "protection of personal information" than current law:</u>
    - Protection = privacy and security protection
    - Personal data = anything that can be used to directly or indirectly a person (including a photo, name, address, location data, IP address, etc.)
    - Sensitive personal information = includes data on racial/ethnic origin, health data, sexual orientation, political opinion, etc. Processing is prohibited except in specific circumstances, requires consent to be lawful.
- <u>Broader consent requirement:</u>
    - Consent must be unambiguous and freely given.

    - Consent must be opt-in (i.e. pre-checked boxes are not GDPR-compliant).
    - Evidence of consent is needed (i.e. lack of response is not enough).
    - Consent must be un-bundled and not incentivized.
    - Withdrawing consent must be possible at any time and as easy as giving
    - The purpose of consent must be clear and specific (in plain language).
- Key Definitions:
    - Data Controller: Decides what data will be processed and how. Typically the school system in ed tech settings. Controllers are liable for the actions of their Data Processor. Controllers are only permitted to engage with GDPR-compliant Data Processors. Controllrs must maintain detailed records of all data processing done on their behalf.
    - Data Processor: Completes data processing operations only as instructed by the Data Controller. Must have the proper technical measures in place to secure data, must delete data promptly, and must maintain thorough records of processing, minimization, and data handling practices.
- Data Subject Rights:
    - Right to be forgotten: Subject may request a company erase or stop disseminating data when it is no longer relevant to the original processing purpose. The Data Controller must compare the subject rights to the rights of the public interest in the data, with a thumb on the scale toward the rights of the data subject.
    - Right to information: Subject may request whether or not, where, and why their data is being processed. Data subjects also have a right to a copy of data held about them and the ability to transmit that data to another Controller.
    - Right to object: Data subjects can object to profiling (i.e. automated processing of personal data to evaluate prospects)
- Enforcement: Conducted by Data Protection Authorities (DPAs) in each member state. DPAs may collaborate on investigations or prosecutions.
- Breach Notification:
    - Data Processors must notify Data Controllers "without undue delay" upon discovery of a breach.
    - Data Controllers must then notify the E.U. supervisory authority within 72 hours of becoming aware of a breach. If this was not possible, the Controller must provide a justification.
    - Data Processors should be very careful not to be a cause of notification delay! There is great exposure here. Clients are already terrified and are requesting heavy indemnities here.
- Penalties: Assessed on a sliding scale encompassing several variables. Penalties are assessed on parent companies.
    - Up to 2% of annual turnover – not handling children's consent, not managing recordkeeping requirements, not conducting PIAs
    - Up to 4% of annual turnover – violating the core principles (which are non-specific!), not respecting individual rights, processing sensitive data without proper consent or authority, transferring data to other countries without proper authority

Compliance Considerations

- Overview
    - Controllers and Processors must demonstrate compliance with GDPR core principles by documenting and enforcing all policies and data protocols and implementing data privacy by design and default
    - Personal data may only be transferred outside the E.U. with appropriate procedures in place. Do due diligence with 3rd parties and subs.
- People and Employment
    - Review training programs and background check protocols for employees
    - Ensure you have the right agreements and documentation in place with your clients (the data controllers)
    - Assess whether you are required to appoint a Data Protection Officer (DPO)
        - Required for those engaged in large-scale, systematic processing and monitoring of personal data, likely including most ed tech companies.
        - DPO must be an expert in your data processes, but they may be staff or a contractor. They must be able to independently perform (i.e. without direction) their job tasks.
        - The DPO must have adequate resources, must report to the highest level of management, and cannot have conflicts of interest. The DPO must have visibility into all processing activities and must make assessments of the necessity and proportionality of processing operations relative to the stated purpose. The DPO is responsible for the organization's compliance with GDPR and should maintain the necessary records.
- Policies & Procedures
    - Ensure you have adequate business processes and standard contractual clauses in place to allow data transfers.
    - Ensure you document and regularly update processes and protocols for all GDPR focus areas
    - Carefully document the implementation of your procedures
    - Conduct due diligence on third-party entities and your sub-contractors
    - Data mapping and system mapping can assist in determining how data is being processed
    - Privacy by design is required and fundamental. Implement correct technical and administrative measures to this effect and record the decisions made throughout this process.
- Products & Services
    - For each product/service, assess data minimization and retention practices
    - For each product/service, assess consent practices and standards (consent must be explicit as to each data processing purpose)
    - For each product/service, assess your security protocols compared to "state of the art" security practices
    - Default settings must be the strictest possible (i.e. everything is private).

Question & Answer

Question: If consent is received to get a service or product, is that considered freely-given?

Answer: It depends. It is generally considered freely-given if you collecting only the data you need to make the product work. For example, collecting an email address when you do not need that information to make your product work is not permitted.

Question: Are GDPR requirements applicable to an entity receiving data from an E.U. controller even when it is just a cross-border transaction and the processor has no E.U. presence?

Answer: Yes. It doesn't matter where the processor is located. If you have information on someone in the E.U., the regulation applies.

Question: Must companies appoint a DPO if they are only getting pseudonymized information?

Answer: The GDPR applies to personal data, so access to only pseudonymized data exempts you from many requirements. You only need a DPO if you are collecting personal information and are above a certain size. If you only get pseudonymized information, you are likely not required to appoint a DPO, especially if you are small and do not collect the more-sensitive types of information.

Attendees

Please email Amelia at avance@fpf.org if you attended this call but your name is not included in the below list.

- 2U
- Colby College
- Data Quality Campaign
- EDUCAUSE
- Institute for Higher Education Policy
- International Association of Privacy Professionals
- Knewton
- National Student Clearinghouse
- New America
- Software and Information Industry Association
- University of California, Los Angeles
- University of Michigan