Should I worry about GDPR?

WITH BRICKER & ECKLER LLP

Bricker & Eckler
ATTORNEYS AT LAW

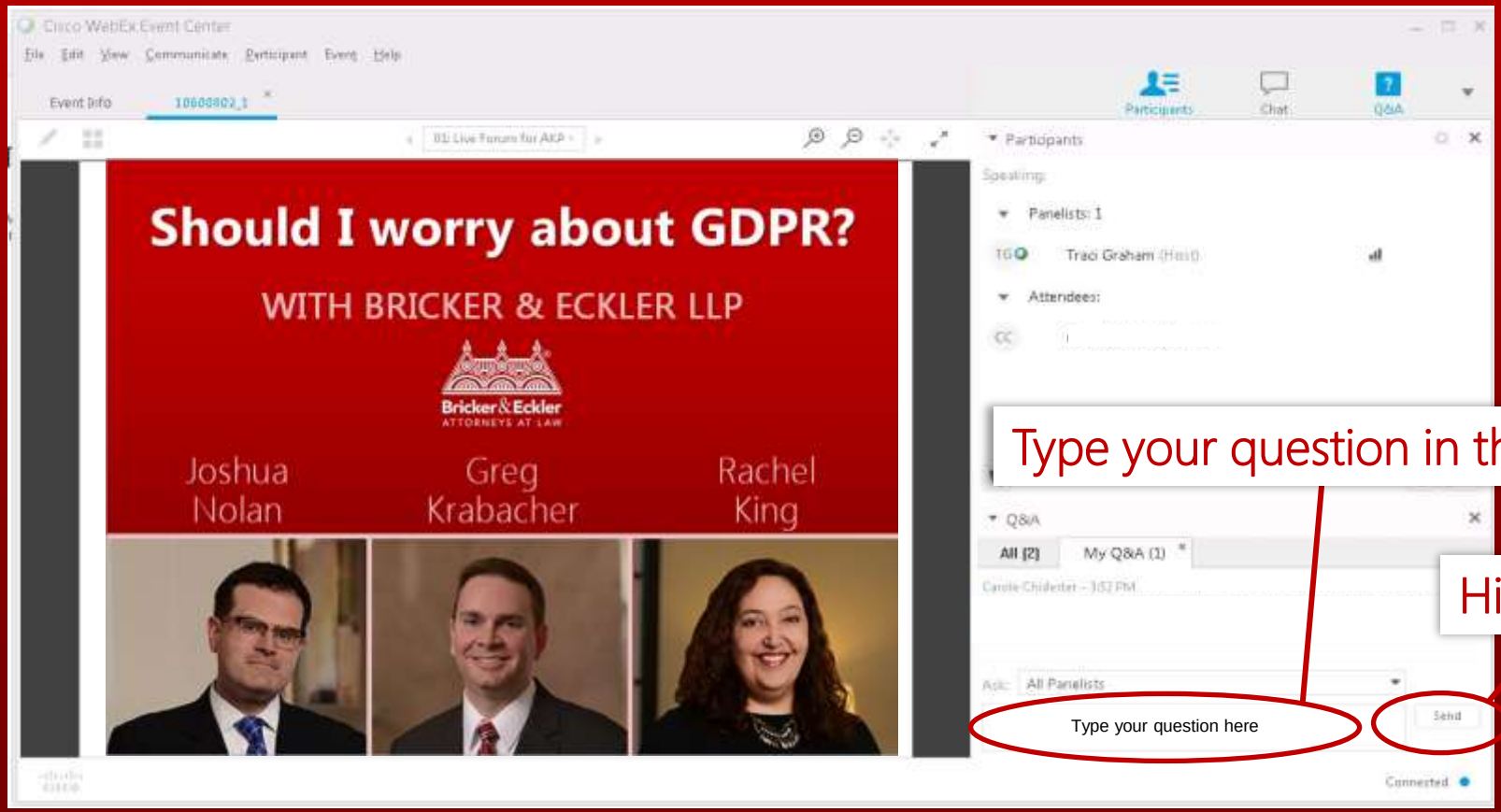
Joshua Nolan

Greg Krabacher

Rachel King

Live Forum

To ask a question using the chat function:



DISCLAIMER

- We are not providing legal advice
- GDPR is new and some questions remain to be answered
- You should always consult with an attorney for any specific legal questions.

What is GDPR?

- The General Data Protection Regulation became effective on May 25, 2018
- Unlike US privacy laws which apply in a particular industry – FERPA, HIPAA, etc. – GDPR applies to all "personal data" that is "processed"
- GDPR's expansive jurisdiction makes it applicable to U.S.-based schools who may not have previously fallen under EU data privacy laws.

Does GDPR apply to my school?

- GDPR applies if any of the following is true:
  - You have a stable presence in the EU – i.e. you have a campus or office in an EU country, or long-term agreements for conducting activities in the EU; or
  - You offer goods or services to individuals in the EU; or
  - You monitor the behavior of individuals in the E.U.

- Note that GDPR jurisdiction is geographical – it applies to all living natural persons physically located in the EU. It is not based on citizenship or residence.
- As a result, it will apply to US students of a US school when those students are in the EU.

What does it mean to "offer goods and services"

Intent is relevant to this prong.

- Merely having a website that can be accessed from Europe does not establish intent;
- Factors that may indicate intent:
  - Local currency, language, or contact info;
  - Specifically targeting EU individuals
  - Using EU gTDLs and internet identifiers

What does it mean to "monitor" behavior?

Intent is not relevant to this prong.

- "Monitoring" not defined in GDPR;
- May include things such as:
  - Online behavioral based advertising
  - Profiling
  - Location tracking

Common IHE activities that implicate GDPR are:

- Accepting admissions applications from the EU – including for on-line courses;
- Running study abroad programs in the EU
- Soliciting donations from EU alumni or other donors

We do all those things - now what?

Now, you need to systematically review the programs in which you "process" the "personal data" of individuals in the EU.

GDPR basics

- GDPR consists of seven core principles, eight individual rights and various other provisions that govern how personal data may be processed.
- Very generally, the purpose is to allow data subjects to control their personal data.

“Personal Data” is:

any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

“Processing” is:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Also…

GDPR further restricts the processing of "special categories" of personal data, which include:

data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

GDPR core principles

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability

Lawful Bases for processing

GDPR specifies which bases are "lawful." Of those, only three are likely to apply to school programs:

1. Consent – must be freely given; can be withdrawn at any time
2. Necessary for the performance of a contract – can include pre-contractual steps, but must be narrowly tailored
3. Legitimate interest – includes marketing and fundraising, must be balanced against privacy interest of data subject

Additional requirements apply …

- When data is transferred to the U.S. – can be done on the basis of a contract with an EU provider, where there is consent or for a contract. Legitimate interest is not a basis.
- When special categories of data are involved – generally requires explicit consent. Legitimate interest is not a basis, nor is performance of a contract, except for employment.

Where do I start?

1. Identify which activities fall under GDPR (admissions, study abroad, etc.)
2. For each, determine what personal data comes from individuals in the EU
3. Determine all the things you do with it

Then…

4. Figure out the lawful basis for processing and whether you are adhering to the core principles;
5. Determine the legal basis for transferring the data to the U.S. (and any separate contracts for this);
6. Notify your data subjects and obtain consent where necessary;

7. Ensure you (“controller”) have adequate contractual provisions for any vendors (“processors”)
8. Establish systems to deal with requests for access, to correct data and to be forgotten;
9. Ensure your security measures are appropriate;
10. Establish a data breach protocol.

Is that it?

No. You need to consider appointing:

- EU Representative (likely); and
- Data Protection Officer (possibly)
  - Yes, if "the processing is carried out by a public authority or body" (per EU nat. law)
  - Yes, if "core activities" involve "large scale" (a) systematic monitoring or (b) processing of special categories of data

You can register for all of our upcoming webinars/events by visiting:

http://www.bricker.com/events/

RACHEL KING
rsking@bricker.com

GREG KRABACHER
gkrabacher@bricker.com

JOSH NOLAN
jnolan@bricker.com - @JoshDNolan

TWITTER
@BrickerHigherEd

TITLE IX RESOURCES
www.bricker.com/titleix

Bricker & Eckler
ATTORNEYS AT LAW