National Association of College and University Attorneys

Presents:

The New EU General Data Protection Regulation: What You Need to Know About It and Why

Webinar

In Cooperation with:

American Council on Education (ACE)
and
American Association of Collegiate Registrars and Admissions Officers (AACRAO)

October 24, 2017

12:00 PM – 2:00 PM Eastern
11:00 AM – 1:00 PM Central
10:00 AM – 12:00 PM Mountain
9:00 AM – 11:00 AM Pacific

Presenters:

Gian Franco Borio
Studio Legale Tributario Internazionale Borio

Bret Cohen
Hogan Lovells US LLP

Stefan Quick
University of Chicago

Contents

NACUA WEBINAR SERIES

Tuesday, October 24, 2017

THE NEW EU GENERAL DATA PROTECTION REGULATION: WHAT YOU NEED TO KNOW ABOUT IT AND WHY

SPEAKER BIOGRAPHIES

Gian Franco Borio, attorney at law and CPA, is Legal Counsel to the Association of American College and University Programs in Italy and to the European Association of Study Abroad. Law degree cum laude from Florence University, specialization studies at SAIS of Johns Hopkins Univ. in D.C., London City Poly, in Germany and France. He served as Technical Counsel for Italy at the Federation of EU CPAs (FEE) to the European Commission on Corporate Law, Tax Law, SMEs. He is admitted to the Florence (Italy) Bar.

Stefan Quick is an Assistant General Counsel at the University of Chicago. His areas of practice include technology transfer, intellectual property, data privacy, information technology and research related matters. Prior to joining the University, Stefan worked as an attorney at McGuireWoods LLP and Davis Polk & Wardwell LLP, specializing in intellectual property, data privacy, and information technology transactions. Stefan holds a B.A. from Northwestern University in Computing and Information Systems and a J.D. from the University of Chicago Law School.

Bret Cohen helps educational institutions, technology companies, and brick-and-mortar businesses comply with privacy, cybersecurity, Internet, and consumer protection laws. He also represents organizations in litigation and government investigations in these areas. As a lawyer and technologist, Bret has a knack for translating legal standards into practical technical requirements that are easy for clients to use.

With a particular focus on the Internet and e-commerce, Bret has advised extensively on legal issues related to data governance, cloud computing, social media, mobile applications, online tracking and analytics, and software development. He counsels and is a frequent speaker on strategic compliance with global privacy laws, such as the EU General Data Protection Regulation, including on topics such as cross-border transfer restrictions, data localization requirements, and government surveillance and requests for information. Bret also spearheads efforts on education privacy, cybersecurity incident preparedness and response, marketing privacy, and workplace privacy.

NACUA WEBINAR SERIES

Tuesday, October 24, 2017

THE NEW EU GENERAL DATA PROTECTION REGULATION: WHAT YOU NEED TO KNOW ABOUT IT AND WHY

ATTENDANCE RECORD

Organization: _____

All participants are asked to sign-in, but if you are an attorney applying for Continuing Legal Education credits (CLEs), you ***must*** sign this attendance sheet to verify your attendance at this seminar. After completion, please return this form to NACUA (clecredit@nacua.org). ***Total CLE Credits = 120 minutes**

	PRINT Your Name	**SIGN Your Name**	**Bar Number** *(If Applying for CLE)*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

NACUA WEBINAR SERIES

Tuesday, October 24, 2017

THE NEW EU GENERAL DATA PROTECTION REGULATION: WHAT YOU NEED TO KNOW ABOUT IT AND WHY

CERTIFICATE OF ATTENDANCE

- **Attorneys from MD, MA, MI, SD, or DC:** These jurisdictions do not have CLE requirements and therefore require no report of attendance or filing.
- **Attorneys from AK, AZ, CA, CO, CT, DE, HI, IL, IA, MN, MO, MT, NH, NJ, NY, TN, WI, or WY:** Do not return this form to NACUA. Please keep this form for your records to submit directly to your state CLE commission or in case your state bar audits you for CLE compliance. Please also remember to sign the site roster, indicating your attendance, before you leave.
- **Attorneys from all other states:** Please complete and return this form no later than TODAY to NACUA (clecredit@nacua.org). Please also remember to sign the site roster, indicating your attendance, before you leave.

NACUA certifies that this program has been presumptively approved and conforms to the standards prescribed by the rules and regulations of the State Bars of AZ, AR, CA, CO, CT, DE, HI, MO, NV, NH, NJ, NM, RI, VT, WV and WY. NACUA will apply for CLE credits from the following states: AL, AK, FL, GA, ID, IL, IN, IA, KY, LA, ME, MN, MS, MT, NC, ND, OK, OR, SC, TN, TX, UT, VA, WA and WI)

NACUA certifies that the New York Approved Jurisdiction policy may apply to this program. New York attorneys may apply CLE credit from one of the approved jurisdiction states towards their NY CLE requirement. For more information and to review the policy, please visit www.nycourts.gov/attorneys/cle/approvedjurisdictions.shtml.

Note: Restrictions vary state by state and not all states will accredit this virtual seminar.

Upon receipt of this certificate of attendance and your site roster, NACUA will process the credits through the applicable state if approved.

CERTIFICATION

By signing below, I certify that I attended the above activity and request 120 minutes of CLE credits.

Name _____ State & Bar Number _____

Address _____ Email _____

Signature _____ Date _____ Verification Code 1 _____ Verification Code 2 _____

(For NY Attorneys Only)

Authorized By:

Meredith L. McMillan

Meredith McMillan, CMP
NACUA: Meetings and Events Planner

The New EU General Data Protection Regulation: What You Need to Know About It and Why

Presented by the National Association of College and University Attorneys (NACUA) in Cooperation with the American Council on Education (ACE) and the American Association of Collegiate Registrars and Admissions Officers (AACRAO)

Gian Franco Borio, Attorney at Law-CPA, Studio Legale Tributario Internazionale Borio

Bret Cohen, Partner, Hogan Lovells

Stefan Quick, Assistant General Counsel, University of Chicago

NACUA | October 24, 2017 Webinar

Agenda

- Overview of the EU General Data Protection Regulation
- Affected University Activities & Strategies for Compliance
- Case Studies
- Question & Answer

Panelists

Gian Franco Borio
Attorney at Law-CPA
Studio Legale Tributario
Internazionale Borio

Bret Cohen
Partner
Hogan Lovells

Stefan Quick
Assistant General Counsel
University of Chicago

General Data Protection Regulation

Background

- **Directive 95/46/EC** (repealed effective May 25, 2018), aimed to harmonize the protection of fundamental rights and freedoms of natural persons with respect to processing activities and ensure the free flow of personal data between Member States.
- **Regulation (EU) 2016/679** (effective May 25, 2018), on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- **Directive (EU) 2016/680** (to be implemented by Member States by May 06, 2018), on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
- **BUT also...** 27 National Legislations to be considered
- And the UK? Same, see: http://www.legislation.gov.uk/ukpga/1998/29/contents

Useful General Web References

- For the full text of the EU General Data Protection Regulation: ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- On EU privacy legislation more generally: http://ec.europa.eu/justice/data-protection/law/index_en.htm
- On Data Protection Bodies in the EU and elsewhere: http://ec.europa.eu/justice/data-protection

Subject-Matter, Objectives and Material Scope of Regulation 2016/679

Key points clarified by articles 1&2 of the Regulation:

- Protection of natural persons' personal data processing and the free movement of their personal data
- These are fundamental rights and freedoms of natural persons
- Union Law to rule and prevail
- Not applicable to the processing of personal data by a natural person in the course of a purely personal or household activity

Subject-Matter, Objectives and Material Scope of Regulation 2016/679

A general principle to be kept in mind, at all times: EU laws always privileges the protection of the **natural person in the union**, irrespective to nationality.

- For U.S. academic institutions, "natural persons" will be:
  - Students (going to study abroad programs in the EU)
  - Faculty (hired locally or posted to the EU)
  - Staff and other personnel (hired locally or posted to the EU)
  - Third parties in general (i.e. local contractors, local donors)

A couple of specific cases, to be discussed:

- International students, located in the EU, applying and then enrolling to U.S. University
- International students, located in the EU, applying and then enrolling to online courses provided by U.S. University

Territorial Scope of Regulation 2016/679

Clarified by Article 3 of the Regulation:

"1. This Regulation applies to the processing of personal data in the context of the activities of an **establishment of a controller or a processor in the Union**, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor **not established in the Union, where the processing activities are related to:**

(a) **the offering of** goods or **services**, irrespective of whether a payment of the data subject is required, **to such data subjects in the Union**; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Territorial Scope of Regulation 2016/679

More concretely:

- US Universities with their own branch campus or study center located in the Union: article 3(1).
- US Universities sending students to or at local counterparts (exchange programs, faculty-led programs, research programs, internships programs): article 3(2).
- US Universities receiving EU students: most likely out of the territorial scope, but still be careful on personal data collection (information onus)

For US study abroad programs in Europe:

www.eu-asa.org

NACUA
National Association of College and University Attorneys
9

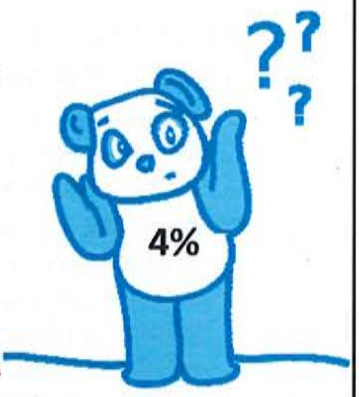
How Does This Impact US Colleges & Universities?

1. US universities with their own branch campus or study center in the EU
2. US universities sending students to or at local counterparts (exchange, faculty-led, research, or internship programs)
3. Collaboration with EU institutions
4. Online learning platforms
5. Research incorporating EU data sets
6. And more...

NACUA
National Association of College and University Attorneys
10

Why Comply?

- **Significant maximum fines**
  - 4% of total worldwide annual turnover or € 20 million, *whichever is higher*
- Requests by EU partners
- Breach notification increases risk of enforcement
- **An accountability-based data governance framework is becoming the global standard of care for privacy**



NACUA
National Association of College and University Attorneys
11

US Privacy Law: A Sectoral Approach

FERPA
FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA

COPPA
Children's Online Privacy Protection Act

NACUA
National Association of College and University Attorneys
12

European Privacy Law: A Comprehensive Approach

- In contrast to the US approach, EU privacy law applies to all "processing" of "personal data"
  - **Personal data**: any information relating to an identified or identifiable natural person (e.g., name, identification number, location data, online identifiers such as IP addresses, images)
  - **Processing**: 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

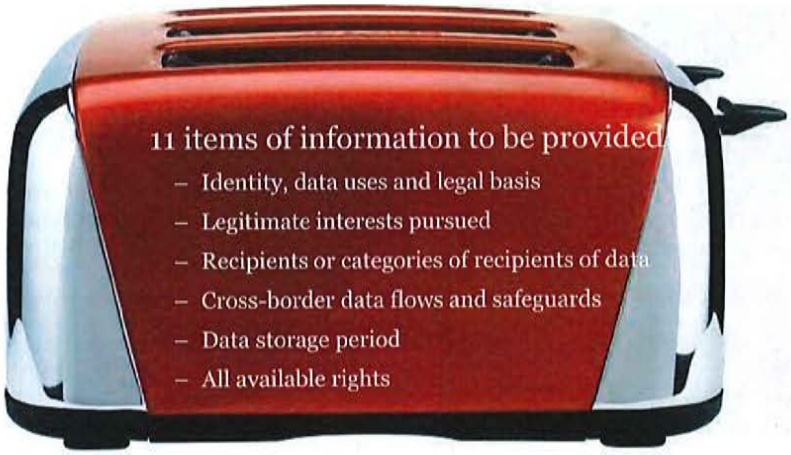
European Privacy Law: The Fundamentals

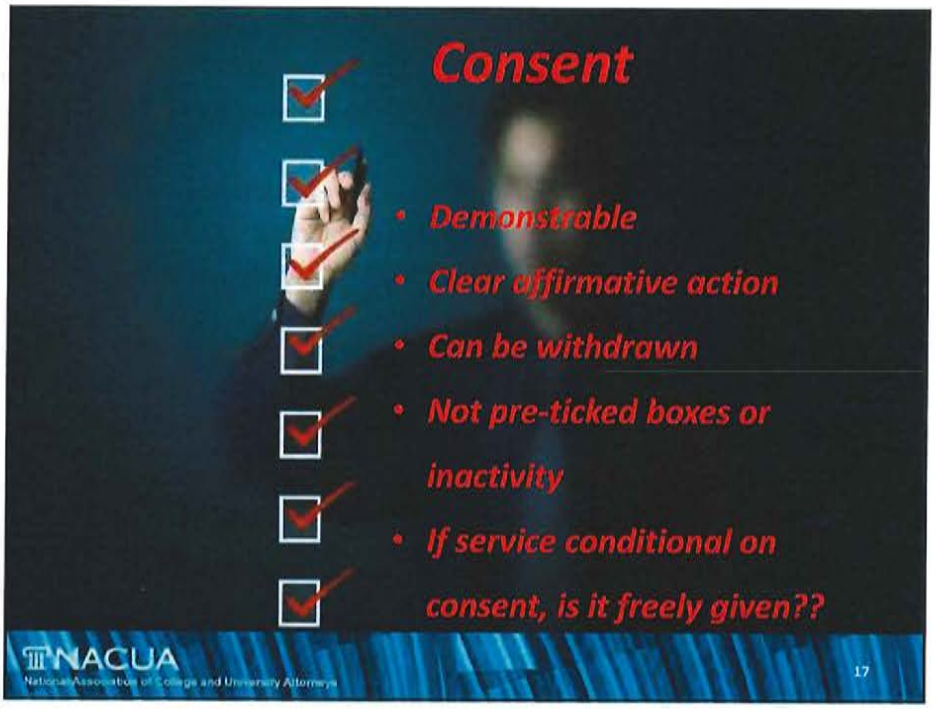
- Data privacy is a **fundamental right**, and cannot easily be bargained away
- There must be a **lawful basis** for all data processing (e.g., consent, necessary to perform a contract, required by law, "legitimate interests" balanced against impact on individuals)
- Personal data processing subject to **principles**: must be lawful, for specified purposes, adequate, relevant, and proportionate, accurate, retained only as long as necessary, secure
- Specific rules for processing **special categories** of personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics or biometrics, health, sex life or sexual orientation, criminal record

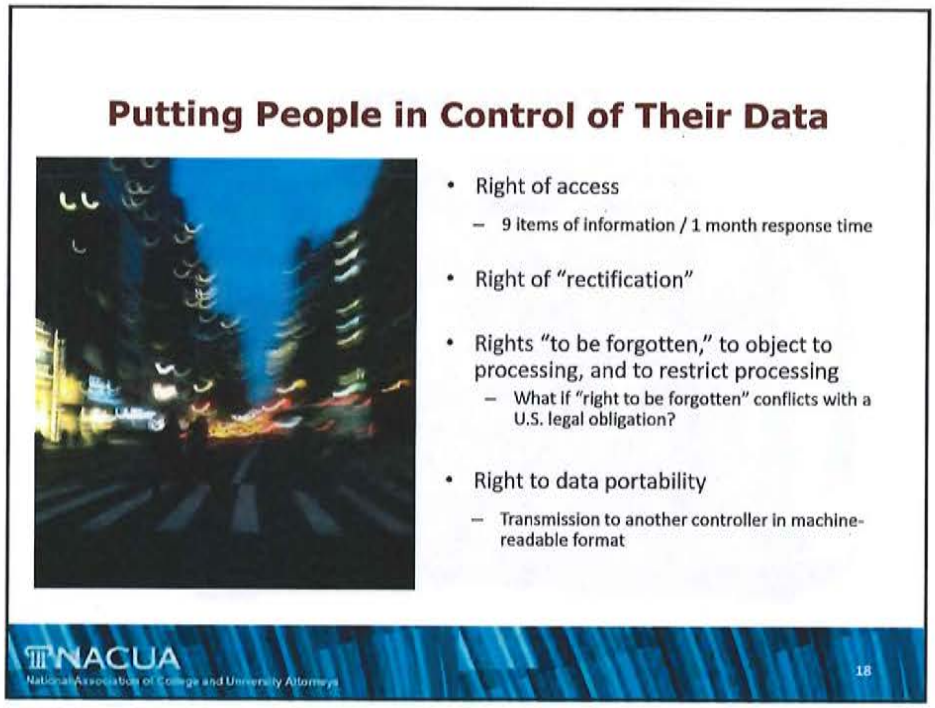
European Privacy Law: The Fundamentals

- Obligations are tied to whether an organization is a "controller" or a "processor" of personal data
  - **Controller**: the entity that determines the purposes and means of the processing of personal data
  - **Processor**: an entity that processes personal data only on behalf of and on the instructions of the controller (e.g., service providers)
- Controllers are subject to significantly more legal obligations under the GDPR
- Processors have some legal requirements, but most obligations will be contractual

Transparency




Consent
• Demonstrable
• Clear affirmative action
• Can be withdrawn
• Not pre-ticked boxes or inactivity
• If service conditional on consent, is it freely given??
NACUA
National Association of College and University Attorneys
17


Putting People in Control of Their Data
• Right of access
– 9 items of information / 1 month response time
• Right of "rectification"
• Rights "to be forgotten," to object to processing, and to restrict processing
– What if "right to be forgotten" conflicts with a U.S. legal obligation?
• Right to data portability
– Transmission to another controller in machine-readable format
NACUA
National Association of College and University Attorneys
18

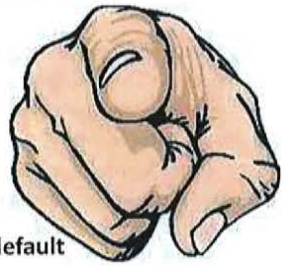
Automated Processing of Personal Data

- "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."
  - Exceptions: necessity to perform a contract, when authorized by EU law, based on explicit consent
- Notice required of "the existence of automated decision-making, including profiling, ... and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

NACUA National Association of College and University Attorneys 19

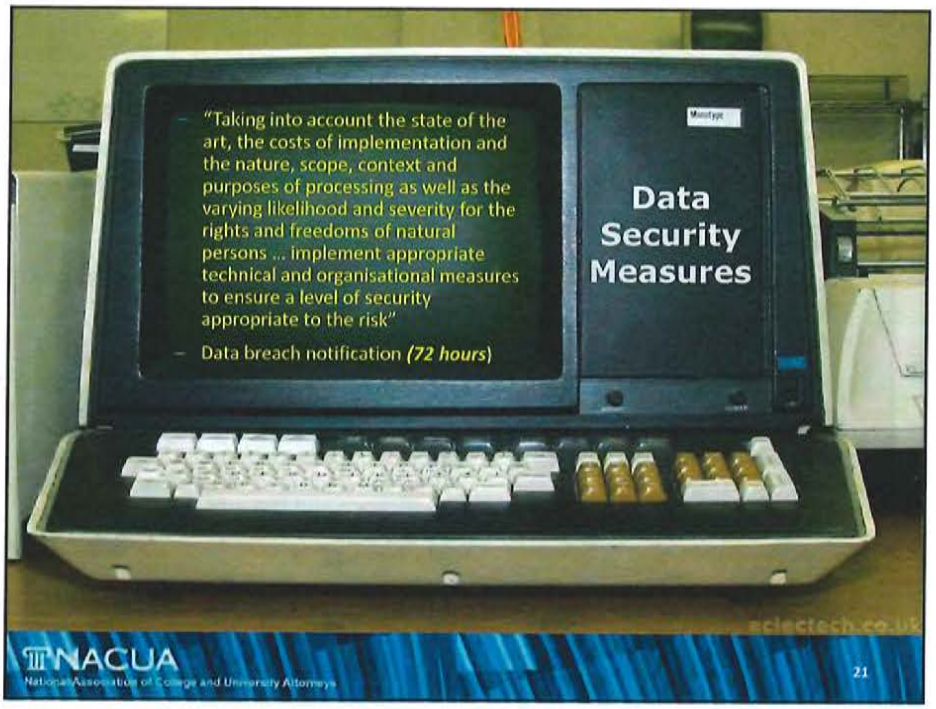
Accountability Obligations

The big novelty & most significant change of the new framework



- Implementation of **data protection policies**
- Data protection **by design** and data protection **by default**
- **Record keeping** obligations
- **Cooperation** with supervisory authorities
- Data protection **impact assessments**
- Prior **consultation** with data protection authorities in high-risk cases
- Mandatory **Data Protection Officers** for certain activities

NACUA National Association of College and University Attorneys 20



Use of Processors / Service Providers

- Appointment by written contract:
  - Only on documented instructions
  - Persons under confidentiality obligations
  - Security measures
  - Sub-contracting conditions
  - Assistance to the controller
  - Deletion or return of data
  - Audit rights

"I like things to be done my way but by somebody else."

- Engagement of sub-contractors:
  - Prior specific or general written authorization by controller
  - Same obligations applicable to primary service provider, which remains liable
- What does this look like under U.S. law? FERPA School Officials

International Data Transfers

- **As a baseline rule, it is unlawful to transfer EU personal data outside of Europe, unless using one of the following mechanisms:**
  - Standard contractual clauses
    - Adopted by European Commission
    - Approved by EU data protection authorities
  - Express consent (which can be revoked)
  - Privacy Shield (cannot be used by non-profits)
  - Binding Corporate Rules

Supervision and Enforcement

- Still national regulators
- Private rights of action
- One-stop-shop?
- Greater international cooperation
- Another new regulatory body: the "European Data Protection Board"

Lawful Bases for Processing

- Consent
- "Necessary for the performance of a contract"
- Necessary for compliance with legal obligation (EU and Member State law only)
- Necessary in order to protect "vital interests" of data subject or natural person (i.e., risk to life or serious harm)
- Necessary for performance of task carried out in public interest or exercise of official authority
- Necessary for legitimate interest, except where such interests are overriden by the interests or fundamental rights and freedoms of the data subject.

Consent

- Consent is not an ideal basis for many institutional activities
- May be revoked at any time
- Cannot be used as "belt and suspenders" with another basis
- Cannot be included in terms and conditions

Necessary for Performance of a Contract

- May apply in some cases
  - Processing for payroll, etc.
  - Admissions?
  - Study abroad?

Necessary for Purposes of Legitimate Interest

- Two part test:
  - Identification of "legitimate interests"
  - Balancing test weighing interests vs fundamental rights and freedoms of data subject
- Discussed at length by Article 29 Working Party in Opinion 06/2014

Legitimate Interest

- Broad definition
- May include:
  - Direct marketing
  - Unsolicited non-commercial messages, including for charitable fundraising
  - Research
- Legitimate interest must be:
  - Lawful (i.e., in accordance with applicable EU and national law)
  - Sufficiently clearly articulated to allow balancing test
  - Represent a real and present interest (i.e., not speculative)

Balancing Test

- Legitimate interest must be balanced against fundamental rights and freedoms of data subject
- Factors to be considered include:
  - Strength of interest (legitimate vs. compelling)
  - Impact on data subjects
  - Transparency and proportionality of measures to protect rights
  - Additional safeguards (e.g., opt out)

Relying on Legitimate Interest

- Notice must specify interest
- Right to object
- Working party recommends documenting analysis
- Least invasive means preferred ('necessary')

Affected Activities and Functions

- EU campuses, affiliates, and programs
- Study abroad
- Development
- Alumni relations
- Admissions
- Online Learning
- Websites & Cookies
- Research
- Procurement

EU Campuses, Affiliates, and Programs

- EU Establishments
  - Not dependent on legal form or physical presence
  - "effective and real exercise of activity through stable arrangements"
  - GDPR covers processing "in the context of" an establishment
  - Model clauses for data transfers to institution
- Study Abroad
  - GDPR applies when students are present in EU

Development, Alumni Relations, Admissions

- Development, Alumni Relations
  - Individual rights: Right to access, Right to be forgotten
  - Provide "opt out"
- Admissions
  - May include special categories of data (e.g., ethnic origin), requiring "explicit consent"
  - Deletion of records

Online Learning, Websites, Cookies

- Online Learning
  - Student data
  - Marketing and advertising activities
  - Review privacy policies, notices, consents for compliance with GDPR
- Websites and Cookies
  - Consider data being collected, manner of processing and use, reasonable expectations of data subject, safeguards
  - Persistent and conspicuous "opt out"

Research

- May include special categories of data
- Consents should be GDPR compliant and compliant with local research laws
- Processing must be proportionate to the aim pursed and provide for appropriate safeguards, particularly data minimisation, pseudonymisation, and deidentification.

Procurement

- Processors must implement appropriate technical and organizational measures
- Contracts must include:
  - Documented processing instructions
  - Flow through obligations to sub-processors
  - Assistance with security and impact assistance
  - Information and audits for compliance
- Further obligations in Article 28

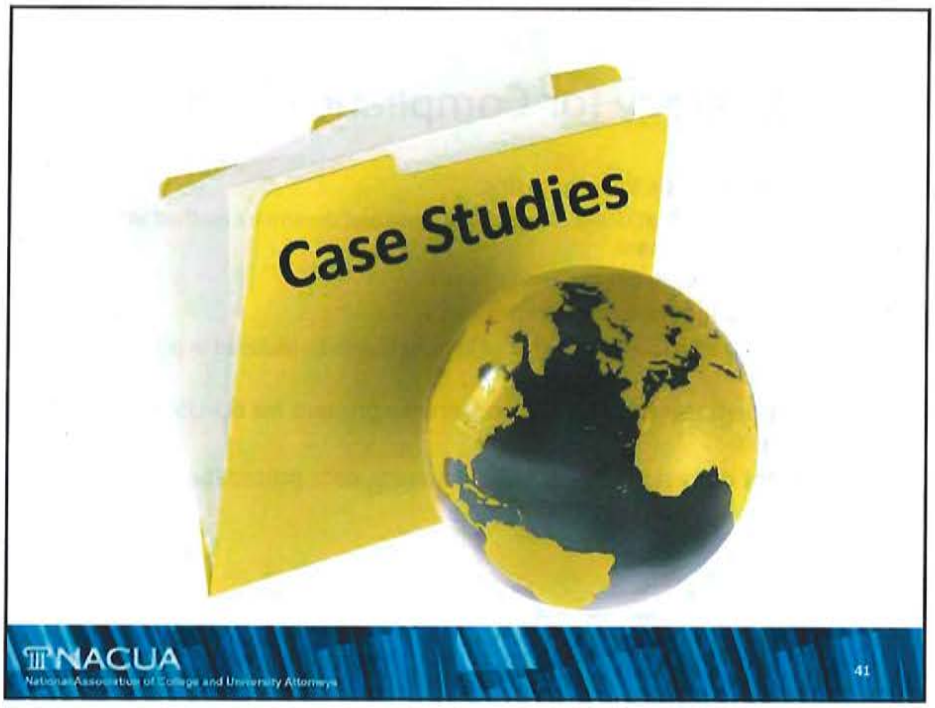
Strategy for Compliance

- Identify impacted offices/units and gather information about activities
  - Study abroad/international office
  - Admissions
  - Alumni relations
  - Development
  - IT

Strategy for Compliance (cont.)

- Determine basis for processing
  - If consent, draft GDPR compliant consent *and* determine method of obtaining consent
  - If other, document basis and analysis
- Revise privacy policies and notices
  - See Articles 13 and 14 for list of information to be included in privacy notices
- Implement model clauses or otherwise prepare for EU-US data transfers
- Appoint representative and, if necessary, data protection officer

Questions & Answers



Case Study 1: Study Abroad Program

- Student A, from US University A, is on a study abroad program in its University located in Venice. Student B, from US University B, is on the same program, thanks to a collaboration agreement between their respective home Universities.
- Student A accuses student B of sexual harassment, files a police claim locally and requests protection. Student B takes local attorney advice, rejects all accusations and files locally a counterclaim for defamation, requesting protection as well.
- Title IX coordinators of both Universities A&B request resident director to immediately act under Title IX applicable provisions.
- The local attorney of student B raises a claim of violation of his client's privacy rights under EU and Italian privacy laws, as resident director transferred personal sensitive data to the US, without his client's prior specific consent and to a potentially unsafe recipient, as University A has not joined the EU-US Privacy Shield.
- Same happens from the local attorney retained by student A.
- Both students then return to their home campuses and respective Title IX procedures take place there, while in Italy the criminal proceedings continue (for sexual violence and defamation)...

Key Considerations

- The resident director is in a no-win position: whatever he or she does or does not do, will violate either EU/local privacy laws or cause the institution to violate Title IX!
- US home institutions need to be aware of this and consider that the territoriality principle governs the case, so EU/local laws will prevail before any EU court or authority
- Negative consequences of such conflict of laws can be minimized by securing the students' prior written consent, under the GDPR rules, to the transfer of their sensitive data to the home office in Title IX situations or the like
- Consent can be withdrawn at any time **but not retroactively!**

Case Study 2: Employee Data

- A University has its own study center in Europe, with both personnel hired locally and U.S.-based faculty that are posted for one or two semesters for various academic purposes (teaching, researching, etc.)
  - Which employees' data are subject to the GDPR?
- The University wants to collect ethnicity and sexual orientation information of faculty for equal employment purposes
  - What steps should the University take?
- Assume there is a dispute between staff that leads to an investigation
  - Can the University apply its standard rules and policies for faculty disputes?
- An employee gets into a dispute with the University, and as part of that says: "I want you to delete all of my data"
  - How should the University respond?

Case Study 3: Scientific Research Project

- US University Alpha entered into a scientific research and test agreement with EU University Beta and EU Institute for Cancer Treatment ("EU Institute"). US University Alpha will provide medical and scientific data/information to EU University Beta and EU Institute on new potential cancer treatments and these will be tested on subjects in the EU. Tests will be performed by EU Institute. Ultimate scientific results will be shared among the three institutions.
- Subjects sign valid consents with privacy waivers that also allow transfer of their personal data to the U.S. Subjects receive some financial compensation from EU institute, which is the recipient of EU Commission public funds for research.
- Tests are performed and results published both in the U.S. and in the EU; however, a dispute arises when a group of subjects claim that the results were published in a way that rendered their identities discoverable.
- A competent national privacy authority and EU Board conclude that (i) processing of personal data was lawful as the "scientific" purpose of that activity was made clear in the consent; (ii) however, the three institutions violated their obligation to take appropriate technical and organizational measures to safeguard the data and comply with the principle of data minimization [see art. 89 of GDPR].

Case Study 3: Key Considerations

- Consents should make clear the scientific (or historical research or statistical) purposes and such purposes should be documented as much as possible
- Even if valid consent is obtained, data security and data minimization principles require safeguarding of information

Case Study 4: Internship Abroad

- Student Y is on a study abroad program in Florence, managed by local art studio school F, under a collaboration agreement with student's US home University. Part of this agreement is that student Y can take a 3-month internship with local fashion company G.
- Local company G requests that the student provide personal information and also some photos, and has him/her sign a waiver form, in Italian. Student G signs, but does not effectively understand that this also means consent to the dissemination of his/her personal data and photos to marketing agencies and the like.
- When his/her photos appear on local magazines and social networks, for advertisement purposes, student Y asks for legal help.
- US University sues the fashion company for violation of Italian privacy laws, but local court rejects its claims, because the violated privacy rights are not the University's but the student's as a natural person. Student Y does not want to continue to pursue the case in Italy.
- US University then sues local art studio school for violation of contractual obligations, because their agreement mandated that local school had the duty to ensure compliance with Italian privacy laws for the University students, but this was not expressly reflected in the subsequent agreement between the local school and the fashion company; University wins damages and legal expense.

Case Study 4: Key Considerations

- Stipulate appropriate contracts with local counterparts, making sure to include privacy rules, and do monitor them!

Questions & Answers

NACUA materials, PowerPoint slides and recordings available as part of this program are offered as educational materials for higher education lawyers and administrators. They are prepared by presenters and are not reviewed for legal content by NACUA. They express the legal opinions and interpretations of the authors.

Answers to legal questions often depend on specific facts, and state and local laws, as well as institutional policies and practices. The materials, PowerPoint slides and comments of the presenters should not be used as legal advice. Legal questions should be directed to institutional legal counsel.

Those wishing to re-use the materials, PowerPoint slides or recordings should contact NACUA (nacua@nacua.org) prior to any re-use.

The New EU General Data Protection Regulation: What You Need to Know About It and Why

NACUA | October 24, 2017 Webinar

Resources

- **General Data Protection Regulation** - *Background* (Slide 4)
  - Directive 95/46/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 (repealed effective May 25, 2018)
  - Regulation (EU) 2016/679: https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en
  - Directive (EU) 2016/680: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG
  - UK Data Protection Act 1998: http://www.legislation.gov.uk/ukpga/1998/29/contents

- **Useful General Web References** (Slide 5)
  - Full Text of the EU General Data Protection Regulation: ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
  - On EU privacy legislation more generally: http://ec.europa.eu/justice/data-protection/law/index_en.htm
  - On Data Protection Bodies in the EU and elsewhere: http://ec.europa.eu/justice/data-protection

- **Territorial Scope of Regulation 2016/679** (Slide 9): For US study abroad programs in Europe: www.eu-asa.org

- **Article 29 Working Party in Opinion 06/2014** (Slide 28): http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

- **Model clauses for data transfers to institution** (Slide 33): http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

- **Additional Resources**
  - AACRAO Trending Topics on GDPR: http://www.aacrao.org/resources/trending-topics/gdpr
  - EDUCAUSE library resources: https://library.educause.edu/topics/policy-and-law/eu-general-data-protection-regulation-gdpr
  - Hogan Lovells, *Future-Proofing Privacy: A guide to preparing for the EU Data Protection Regulation*, https://www.hoganlovells.com/en/blogs/fintech-blog/future-proofing-privacy
  - Hogan Lovells *GDPRnow*, a mobile application that provides companies with assistance to identify practical steps to comply with the new framework. Download instructions available at http://www.hldataprotection.com/2017/05/articles/news-events/hogan-lovells-launches-gdprnow-app.

EU GENERAL DATA PROTECTION REGULATION QUESTIONNAIRE

From and after May 25, 2018, some of the institution's activities will be subject to new and more stringent regulations governing the use of personally identifiable information. The new European General Data Protection Regulation, or "**GDPR**" imposes new obligations on entities that control or process personally identifiable information about people in Europe.

Unlike the current European data privacy regulations, the new regulations apply to entities, like our institution, that are located *outside* of Europe. In addition, the regulations apply to data about *anyone in Europe*, regardless of whether they are a citizen or permanent resident of a European Union country.

Among other things, the GDPR requires an organization to:

- appoint a person to oversee data protection activities;
- be transparent about the personal information it collects and the uses it makes of any personal information;
- keep track of all uses and disclosures it makes of personal information;
- ensure that all vendors and third parties to which it provides personal information have adequate privacy and security protections; and
- enter into special terms when transferring personal information to certain other jurisdictions (including the United States).

The GDPR applies to the processing or control of 'personal data.' The law defines 'personal data' as follows:

> 'personal data' means 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;

If we are storing, processing, or otherwise utilizing any 'personal data' of individuals in Europe, we will need to understand how and why and make sure we comply with the new law.

We have prepared the attached questionnaire to facilitate further discussions about what steps, if any, the institution may need to take to comply with the new law in your area. We ask that you respond to each question to the best of your knowledge. One to two sentence answers will be most helpful in guiding our future discussions. After receiving your response, we will contact you to set up a time to discuss the information you provided and develop a more detailed plan to comply with the new law.

Should you have any questions about this. Please feel free to contact any of the persons listed below.

1. Organizational Information

   a. Name of Unit/Department:

   b. Who in your Unit/Department will be responsible for GDPR compliance?

2. Scope of Personally Identifiable Information

   a. Do you maintain information about European residents or others who are permanently or temporarily located in Europe? If so, please describe.

   b. Do you have employees located, permanently or temporarily, in Europe or who regularly travel to Europe? If so, please describe.

   c. Do you have students located, permanently or temporarily, in Europe or who travel to Europe as part of a program? If so, please describe.

   d. What personally identifiable information do you maintain or use in your EU-related activities? Examples include student data, employee data, data about alumni and donors, and applicant data. Please note that you only need to specify *identifiable data*, so if the data you maintain or use cannot be used to identify a specific individual, you do not need to list it. Please list types of data by activity.

Activity	*Type of Personal Data*

      i. Do you receive this information directly from individuals or do you receive it from third parties?

         (1) If you receive this data from individuals, do you obtain their affirmative consent when you do so? If so, please provide the consent you use or describe the process.

            (a) Do you retain copies or records of the consents you obtain?

         (2) If you receive this data from third parties, please list the third parties below and provide the contracts under which you receive this data.

      ii. Do any of our websites collect personal information from visitors – either automatically or through forms filled out by visitors?

         (1) If so, do you have a privacy policy posted on our website?

         (2) Do you notify visitors of the ways in which you use their data?

         (3) Do you ask visitors to consent before you collect their data? If so, please provide the consent you use or describe the process.

(4) Do we use cookies to collect identifiable information (IP addresses, names, etc.)? If so, what information?

(a) Do you retain copies or records of the consents you obtain?

iii. Do you collect, store, or use any of the following types of data about individuals from the EU:

(1) Racial or ethnic origin;

(2) Political opinions;

(3) Religious or philosophical beliefs;

(4) Trade union membership;

(5) Genetic or biometric data;

(6) Health data;

(7) Sexual orientation; and

(8) Criminal convictions or offences.

3. Use of Personally Identifiable Information

a. How do you use the personal information you have and why? For example, you use employee data to pay employees and you use student data to track student performance, manage student housing, etc.

Type of Personal Data	*Use*	*Reason for Collecting/Using Data*

b. Do you have a written privacy policy regarding our use of personally identifiable information?

i. If so, please provide a copy of the policy.

c. Do you provide notice to individuals regarding how you use their personal information?

i. If so, please describe the process for notification and the contents of the notice?

4. Response to Individual Requests

a. How do you respond to requests from individuals about their data?

b. Do you permit them to amend the data you have about them?

c. Do you delete their information if they request that you do so?

i. Do you contact our third-party vendors and other areas of the institution and ask that they comply with the request?

5. Administrative Requirements

   a. Do you have an individual that is responsible for data privacy matters?

6. Data sharing

   a. Do you share any personal information with third parties? For example, do you have vendors to whom you provide personally identifiable information?

      i. If so, please provide any contracts with those vendors.

   b. Do you transfer any personal data from Europe to other countries?

      i. If so, to what countries and to which entities/persons in those countries?

   c. Do you transfer any personal data from the United States to any other non-EU countries?

      i. If so, to what countries and to which entities/persons in those countries?

7. Data Security and Access Restrictions

   a. How do you store personal information?

      i. Is personal information encrypted?

      ii. Are identities obscured through the use of aliases or alphanumeric unique identifiers?

   b. When you transmit or transfer personal data, do you do so securely (i.e., by encrypting the data while in transit)?

   c. Is access to personal data restricted to only those who "need to know" such personal data?

      i. If so, what technical measures are in place to enforce such restrictions (e.g., restricted access permissions, password protection, etc.)?

8. Breach Response

   a. Do you have a documented policy, process, or procedure for responding to data security/privacy incidents?

GDPR COMPLIANCE CHART

Enterprise Wide Issues:

ISSUE	DESCRIPTION	PLAN
Appointment of DPO	Article 37 requires organizations to appoint a DPO in certain cases.	
Appointment of Representative	Article 27 requires controllers and processors not established in the Union to appoint a representative.	
Standard Contract Clauses for Downstream Processors/Vendors	Article 28 requires contracts with processors to comply with certain requirements.	

Potentially Relevant Activities:

ACTIVITY	TYPE OF DATA	LAWFUL BASIS	COMPLIANCE PLAN
Foreign Travel			
Study Abroad	PD of students		
Sponsored Travel	PD of faculty, staff, and students		
European Centers/Activities			
EU Centers/Activities	PD of employees		
	PD of students		
	N/A		
Student Data			
Admissions	PD of applicants		
Alumni	PD of alumni		
Donors	PD of donors		
Career Services	PD of students and alumni		
Student Records	PD of students and alumni		
Medical Records/SCS	PD of students and alumni		
Online Learning			
EU Student Data	PD of online learners		
Employment Data			
Staff Employment Applications	PD of applicants		
Academic Employment Applications	PD of applicants		
Research			
Research Data Sets	PD of EU research subjects		
Research Conducted in EU	PD of EU research subjects		
	PD of study personnel in EU		
Websites			
Websites with Cookies	PD of website visitors		
Marketing and Outreach			
Advertising emails/messages	PD of recipients and responders		