International Privacy Laws: Those New EU Data Protection Regulations Do Apply to You!

The Forum on Education Abroad
Thursday, March 22, 2018

Presented By:

Gian Franco Borio, Legal Counsel to the Association of American College and University Programs in Italy (AACUPI) and to the European Association of Study Abroad (EUASA)

William P. Hoye, EVP, General Counsel and Chief Operating Officer, IES Abroad

GOALS

You Should Leave Today's Session With:

1. A deeper understanding of the new GDPR Regulations;
2. A better idea of how the new regulations are likely to apply on your campus and to your programs, activities, and operations in EU Countries;
3. Greater awareness of how to pro-actively avoid missteps that could result in privacy violations, large fines, and potential legal liability in the future; and,
4. Some practical tips for complying with the new GDPR regulations which can be accomplished in a number of ways:
    a) Getting written consent that freely given, specific, informed and unambiguously given from a student faculty member or staff member
    b) As with FERPA, the new GDPR regulations also contain an emergency exception where disclosure or use of sensitive data is necessary to protect vial interest of your student, faculty, staff member, etc.
    c) There's also an exception to the restriction on processing sensitive data when necessary to carry out obligations in the field of employment

GENERAL DATA PROTECTION REGULATION (GDPR) BACKGROUND AND INFORMATION SOURCES

- **Directive 95/46/EC** (repealed effective May 25, 2018), aimed to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and ensure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.

GENERAL DATA PROTECTION REGULATION (GDPR) BACKGROUND AND INFORMATION SOURCES *(Continued)*

Also, 27 National Legislations to be considered

And the UK? See :

http://www.legislation.gov.uk/ukpga/1998/29/contents

USEFUL GENERAL WEB REFERENCES:

For the full text of the new EU General Data Protection Regulation:

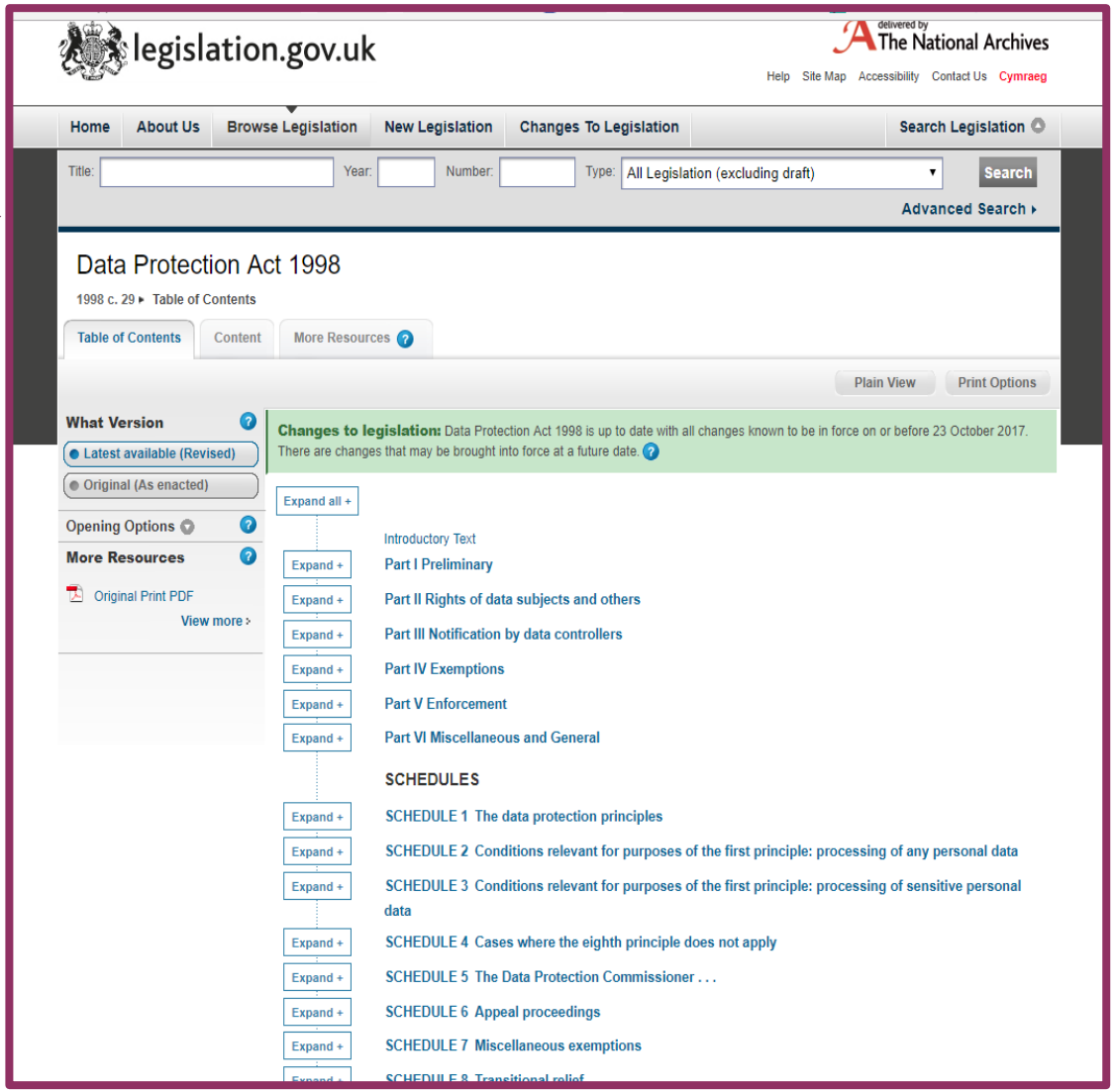
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

General EU privacy legislation:

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/bodies/index_en.htm



SUBJECT-MATTER, OBJECTIVES AND MATERIAL SCOPE OF REGULATION 2016/679

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

1. Protection of natural persons' personal data processing and the free movement of their personal data.
2. These are fundamental rights and freedoms of natural persons.
3. Union Law to rule and prevail.
4. 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 *(CONTINUED)*

A general principle to keep in mind, at all times:

1. EU laws shall always privilege the protection of the **natural person in the union**, irrespective to nationality.

2. For the U.S. academic institutions, "natural persons" will be:

   a) Students (attending study abroad programs in the EU)

   b) Faculty (hired locally or posted to the EU)

   c) Staff and other personnel (hired locally or posted to the EU)

   d) Third parties in general (i.e. EU contractors, EU donors, EU researchers)

Specific cases, to be discussed:

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

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 behavior as far as their behavior takes place within the Union.

TERRITORIAL SCOPE OF REGULATION 2016/679 *(CONTINUED)*

Clarified by Article 3 of the Regulation:

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."

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, protection)

KEY DEFINITIONS

1. **Personal Data**: 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.

2. **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, restrictions, erasure or destruction;

KEY DEFINITIONS *(CONTINUED)*

3. **Profiling:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
4. **Controller:** the natural person or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data;
5. **Processor:** a natural person or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
6. **Consent** (of the data subject): any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or to her;
7. **Personal Data Breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

According to Article 5 of the GDPR, the following general principles shall have to be fully respected by the organization (i.e. the University) collecting, processing and storing personal data:

A. Lawfulness, Fairness, and Transparency
B. Purpose Limitation
C. Data Minimization
D. Accuracy
E. Storage Limitation
F. Integrity and Confidentiality
G. Accountability

SENSITIVE DATA: HIGHER PROTECTION *(i.e., Handle With Care)*

Sensitive Data Definition: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.

Key Rule: Their processing is prohibited unless:

- Explicit consent of the data subject (will be main case);
- Necessary to carry out obligations in the field of employment, social security, etc. (will also be quite utilized);
- Necessary to protect vital interests of the data subject (emergency situations);
- Others (exercise legal defense, data made public by data subject, substantial public interest, preventive or occupational medicine, public health); and,
- Necessary for achieving purposes in the public interest, scientific or historical research purposes, provided that it shall be proportionate to aim pursued and safeguards the fundamental rights of the data subject.

RIGHTS OF THE DATA SUBJECT = RESPONSIBILITY OF ORGANIZATION

- Full and transparent information and communication
- Right of access
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not to be subject to automated individual decision-making, including profiling

RIGHTS OF THE DATA SUBJECT = RESPONSIBILITY OF ORGANIZATION *(CONTINUED)*

Consequential organization responsibility as data controller:

Article 24: "Taking into account the nature, scope, contest and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedom of natural persons, the controller shall **implement appropriate technical and organizational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

Article 25: Data Protection by Design and by Default

Need of the implementation of appropriate technical and organizational measures (such as pseudonymisation and data minimization) to meet the GDPR requirements

RIGHTS OF THE DATA SUBJECT = RESPONSIBILITY OF ORGANIZATION *(CONTINUED)*

But, what these technical and organizational measures are and how to achieve them is left to the organization!

It will be up to the IT specialists to define and implement these measures. Then, the organization has the responsibility to perform self assessment procedures.

Here are two main GDPR requirements that will have to be implemented…

RECORDS OF PROCESSING ACTIVITIES – DATA BREACH NOTIFICATION AND COMMUNICATION

A. **<u>Records of Processing Activities</u>**: each controller/processor shall maintain a record of processing activities, containing key information such as purposes of data processing, data subjects and personal data categories, data recipient's categories, data transfers to non-EU countries, time limits for data erasure, description of technical and organizational security measures.

Records shall be in writing, which includes both print and electronic, and shall be made available to supervisory authority on request. Possible exemption from such record keeping occurs if an organization employs fewer than 250 persons. However, if sensitive data is processed, there is no exception.

RECORDS OF PROCESSING ACTIVITIES – DATA BREACH NOTIFICATION AND COMMUNICATION (CONTINUED)

B. **Personal Data Breach**: in the case of a personal data breach, controller shall immediately (not later than 72 hours) notify it to the national supervisory authority, with specific information to be provided.

Moreover, when such a breach is likely to result in a high risk to the rights and freedoms of natural persons, controller shall communicate it to the data breach with undue delay. Such communication shall not be required if appropriate technical and organizational protection measures have been implemented so that personal data are unintelligible to unauthorized parties (such as encryption); same if subsequent measures are taken so that the high risk to rights and freedoms is no longer likely to materialize or if there would be a disproportionate effort.

All above leads to the recommendation that any organization subject to the GDPR duly performs a sincere data protection impact assessment, whose guidelines are stated in article 35 (7); and to designate a data protection officer (DPO), whose duties are stated in article 39.

DPO: THE GDPR KEY FIGURE

- The DPO is to be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the mandated tasks.

- DPO may be a staff member of the organization or a third party contractor. In either case DPO will have to be and remain fully independent in performing his or her tasks, bound to full confidentiality, and shall not be dismissed or penalized by controller/processor for performing his or her tasks.

- DPO shall perform the following tasks:
  - Inform and advise of the legal obligations related to personal data processing, arising out from the GDPR and any applicable national law;
  - Monitor compliance with GDPR and other applicable data protection provisions, as well as with any existing policy of controller/processor;
  - Provide advice where requested on data protection impact and monitor related performance;
  - Cooperate with competent national supervisory authority;
  - Act as contact point with such supervisory authority.

Conclusion: it is easy to predict that **DPO function will normally be assigned to an IT specialist,** as it has already been the rule under the current privacy data EU and national norms.

Key Question: Is the DPO always mandatory? Maybe not….

REPRESENTATIVE OF CONTROLLERS OR PROCESSORS NOT ESTABLISHED IN THE UNION

In the situation governed by Art. 3(2) [i.e. the U.S. Institution does not have its own direct establishment in the EU, but is offering services to individuals in the territory of the Union: faculty-led programs is the key example], **A dedicated local privacy representative is to be designated in writing (art. 27).**

Possible exemptions Include:

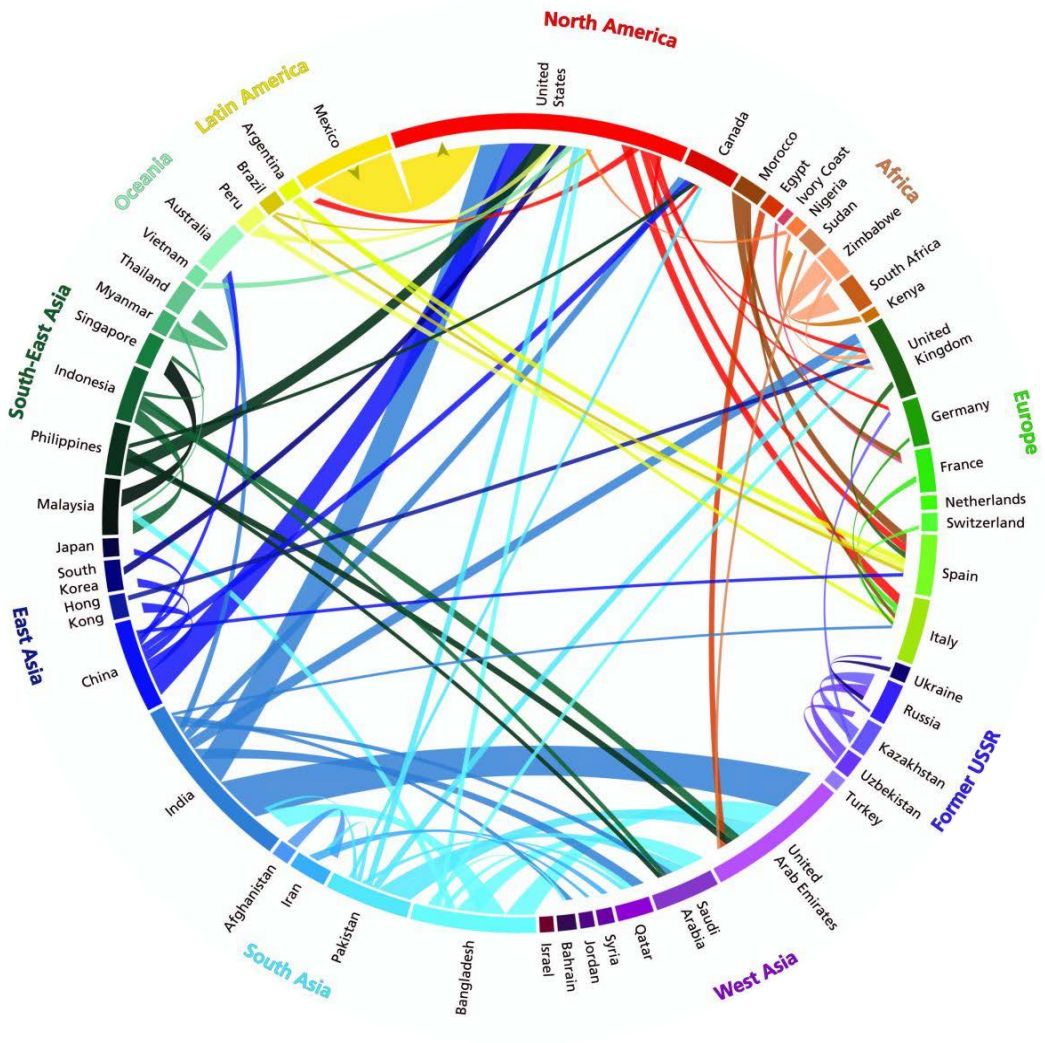
- When processing is occasional or does not include a large scale processing of sensitive data AND is unlikely to represent a risk to the rights and freedoms of the individuals, all taken into due account…[so, probably, a "small" Summer Program could be exempted…];
- Representative to be established in one of the EU Member States and can of course cover more Member States;
- Representative will act on behalf of the U.S. institution, so appropriate contractual arrangements will be required (specific duties, compensation, dispute resolution, etc.);
- Purposes of designation are ensuring compliance with the GDPR;
- Representative designation does NOT relieve the U.S. institution from its own legal responsibilities under the GDPR; or,
- Representative will be the point of immediate reference for local supervisory authorities and data subjects.

Who is going to be appointed? Local counterparts (providers)? Local IT experts? Local law firm?

FLOW OF INFORMATION BETWEEN THE EU AND THE US

- Relatively easy until 2015: in EU Commission Decision 2000/520/EC, the "Safe Harbor Privacy Principles" implemented in accordance with the guidance provided by the so-called "FAQ" issued by the US Department of Commerce, were considered to ensure an adequate level of protection for personal data transferred from the Union to organizations established in the United States.

- Then, in its judgment of 6 October 2015 in Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, the Court of Justice of the EU declared Decision 2000/520/EC invalid, because it considered that the Commission had not stated that the US in fact "ensured" an adequate level of protection by reason of its domestic law or international commitments.



FLOW OF INFORMATION BETWEEN THE EU AND THE US (CONTINUED)

- This caused a kind of "limbo" situation, while anyway since 2014 the EU Commission had entered into talks with the US authorities in order to discuss the strengthening of the Safe Harbor scheme; after Schrems, these negotiations were intensified and have led to EU Commission Decision 2016/1250 of July 12, 2016, by which the Commission has approved the EU-US Privacy Shield.

- Privacy Shield is based on a system of self-certification by which US organizations commit to a set of privacy principles (called the EU-US Privacy Shield Framework Principles, including Supplemental Principles), issued by the US Department of Commerce.

- US Universities should therefore join the Privacy Shield Program as administered by the US Department of Commerce, see: www.commerce.gov/page/eu-us-privacy-shield and www.privacyshield.gov.

Not possible? EU authorities will solicit the creation of a Privacy Shield Program designed for nonprofit organizations!

FLOW OF INFORMATION BETWEEN THE EU AND THE US (CONTINUED)

In the absence of that, article 49 of Regulation 2016/679 allows a transfer or a set of transfers of personal data to a third country, if:

A. **The data subject has explicitly consented** to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the (possible) absence of appropriate safeguards.

B. The transfer is necessary for the performance of a contract between the data subject and the controller [***Caution***: this may work for students going to the EU, not for local staff or faculty under a local contract, as transfer of their data to the US is not necessary to perform their contract, legally speaking].

C. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person [it may work in the cases of internship agreements, research agreement].

FLOW OF INFORMATION BETWEEN THE EU AND THE US (CONTINUED)

D. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent. [this is the case of "emergencies situations", where privacy rights can be derogated at any time. But, the emergency situation needs to be real and the University may then be called to prove it]

Conclusion: Seriously consider having your client join the Privacy Shield Program! **But,** keep in mind that the US Privacy Shield is tailored for business entities and not accessible to Universities. EU authorities may wonder why and solicit the US nonprofit organizations to build their own Privacy Shield (for example under the Department of Education).

OTHER LAWFUL POSSIBILITIES:

1. Adopt the so-called Standard Contractual Clauses as adopted and approved by the EU authorities. This option is possible but difficult (see http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).
    a) Note: One cannot contract with him/herself!
2. Adopt the so-called Corporate Binding Rules, namely a kind of "Privacy Code of Conduct". Something like this is certainly possible, however, it is highly complex, time-consuming, and expensive to achieve. Given the mandatory requirements and procedure that are to be followed to have them accepted by the EU/national Privacy Authorities; see: http://194.242.234.211/documents/10160/10704/443954.
    a) Note: the Corporate Binding Rules have proven to be effective for big multinational business undertakings, rather than for Higher Ed Institutions.

CONCLUSION:

As on today, the safest solution, from the EU perspective, remains to secure the appropriate "freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data related to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website. It should be noted that silence, pre-ticketed boxes, or inactivity [do] not therefore constitute consent.

If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

[GDPR, Whereas #32]

SAME NOTICE & CONSENT DOCUMENT CAN INCLUDE:

- General consent to personal data collection, processing and storage
- Specific consent to personal sensitive data collection, processing and storage
- Specific consent to personal data transfer from the EU to the U.S.
- Dedicated consent for the purposes of Title IX situations

FREQUENTLY ASKED QUESTIONS ON CONSENT:

- When Should Consent Be Collected?
  - Ideally, consent should be collected before leaving the home campus.

- What About Consent Withdrawal?
  - Consent can be withdrawn by the data subject at any time, even if the request is only done orally. However, withdrawal is **NOT** retroactive.

- What If Consent Is Not Given?
  - That becomes a risk management decision: is the institution ready to run the risk of potential claims for damages or for personal data breaches?

REMEDIES, LIABILITIES AND PENALTIES

1. Right to lodge a complaint with national supervisory authority (art. 77): this will be regulated by domestic law of the Member State of the complainant's habitual residence, place of work, or place of the alleged infringement. In some countries, this may lead to financial penalties and there will be a very negative impact on the media.
    a) Against any binding decision of a supervisory authority natural and legal person will always have an effective judicial remedy according to applicable Member State law.

2. Right to an effective judicial remedy against a controller or a processor (art. 79): each data subject has the right to an effective judicial remedy whenever he or she believes that his or her rights under the GDPR have been infringed by a controller or/and a processor. Proceedings shall be brought before the courts of the Member State where controller or processor has an establishment; alternatively, before the courts of the Member State where the data subject has his or her habitual residence.

3. Right to compensation for damages (art. 82): any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from controller and /or processor. Court proceedings shall be before the courts competent under the law of Member State of establishment or habitual residence.

4. Administrative fines (art. 83): general conditions for imposing administrative fines by either the supervisory authority or the national courts are listed. The most serious infringements (such as violating the basic principles for processing, including conditions for consent, violating the data subject's fundamental rights, violating the rules for the transfers of personal data outside the EU), shall be subject to fines up to 20 million euro or up to 4% of the total worldwide turnover of the preceding financial year, whichever is higher.

CONCRETE CASE #1: STUDY ABROAD PROGRAM

Student A, from US University A, is on a study abroad program at 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).

CONCRETE CASE #1: STUDY ABROAD PROGRAM *(CONTINUED)*

- And the loser is….
- And the solution would have been…..

CONCRETE CASE #2: EMPLOYMENT DISPUTE

State University X has its own study center in Rome, duly established and authorized to operate as a nonprofit academic entity, with personnel hired locally (staff & faculty).

University X also posts home-hired faculty to this study center, to perform for one or two semesters a variety of academic activities (teaching, researching, etc.).

Home faculty H raises the claim of insubordination and verbal violent behavior against local staff member K. Local staff member K counterclaims that home faculty H has committed acts of violence against him/her.

University X HR office issues an order of suspension from service to both individuals and sends an investigation team to Rome. Hearings are held in Rome, following University X rules and policies.

Local staff member K retains local attorney who gets an urgency order from local labor court to stop such investigation process and then sues University X for damages and other labor claims. A specific report is also sent to the Italian Privacy Authority, which opens a file against University X for violation of privacy rules, as personal sensitive and labor data of both involved individuals have may have been violated.

Labor case with employee K is then settled before the local labor court, quite expensively for the University, privacy case ends up with a fine of 15,000€.

CONCRETE CASE #2: EMPLOYMENT DISPUTE *(CONTINUED)*

- Lesson to Learn: always check with local (University) attorney on local labor and privacy laws before taking any action and do not pretend that US laws, procedures and practice can be automatically applicable in another sovereign country.

CONCRETE CASE #3: 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 the student to 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 pursue the case in Italy and lets the whole matter drop.

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 expenses!

CONCRETE CASE #3: INTERNSHIP ABROAD *(CONTINUED)*

- Lesson to Learn: stipulate appropriate contracts with local counterpart, making sure to include privacy rules, and do monitor them!

CONCRETE CASE #4: SCIENTIFIC RESEARCH PROJECT

US University Alpha has stipulated a scientific research and test agreement with EU University Beta and EU Institute for Cancer Treatments. The US University will provide medical and scientific data/information to both the EU University and Institute on new potential treatments against cancer. This data will be tested on voluntary patients based in the EU and the tests will be managed by the EU Institute. The final scientific results will be shared among the three institutions.

Voluntary patients sign due hold harmless releases to all three institutions and specific privacy waivers that allow the transfer of their personal/sensitive data to the U.S. Voluntary patients are to receive a form of financial compensation from the EU institute, which is the recipient of EU Commission public funds for research.

Tests are performed and the results are published both in the U.S. and in the Union. However, a dispute arises as a group of patients claim that, irrespective to their initial consent, some of their personal data (first names, dates of birth, ethnical origin) were not to be disclosed to the (scientific) public at large, both in the U.S. and in the Union.

Competent national privacy authority and EU Board come to the conclusion that (i) processing of patients' personal data was lawful as the "scientific" purpose of such activity was very clearly outlined, explained and then effectively performed; (ii) however, the three institutions had to take appropriate technical and organizational measures to safeguard the principle of data minimization [see art. 89 of GDPR], so that identification of data subjects could have been avoided.

CONCRETE CASE #4: SCIENTIFIC RESEARCH PROJECT *(CONTINUED)*

- Lesson to Learn: Detail the scientific (or historical research or statistical) purposes of any agreement of this kind with EU institutions as much as possible. You should duly monitor their achievements and reduce data handling as much as possible.

QUESTIONS?


Thank you