University of Padova
Course of Law and Data
Academic Year 2021-2022
Instructor: Elisa Spiller, Ph.D.

1st Exam Session | January 26th, 2022

*Instructions*

- ❑ Write your answers using an ***intelligible handwriting***
- ❑ Write your ***name***, ***surname*** and ***student number*** on the top of the answers' sheet

*Part 1 – Multiple choice questions*

1. *Which of the EU institutions is regarded as the Guardian of the Treaties and EU Law?*
   a. The European Parliament
   b. The European Commission
   c. The European Court of Justice

2. *Which is not a function of the Court of Justice of the European Union (CJEU)?*
   a. The consistent interpretation of European Union law
   b. Consideration of the validity of the acts of the Institutions
   c. Hearing appeals from national courts

3. *Which of the following statements best describes what the General Data Protection Regulation is?*
   a. An update on the Directive 95/46 which means personal data can only legally be collected and stored by companies that are certified in accordance with the GDPR regulations
   b. A legal framework aimed at companies operating online in the EU, stipulating how and when companies are able to collect personal data
   c. A legal framework relating to the collection, storage and usage of personal data, which applies to any organization doing business with EU citizens

4. *What are the types of personal data as defined under GDPR?*
   a. Any identifiable information
   b. Only name, identification number, location data, online identifier, specific factors related to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person
   c. Personally identifiable information & special categories of personal data

5. *Which of the following is not an example of a special category of personal data?*
   a. Ethnicity
   b. Religious beliefs
   c. Date of Birth

6. *Considering the decision of the EUCJ on the Google Spain case, which of the following statements is correct:*
   a. When there are insufficient legal references, the EUCJ has unlimited power in creating new rights to address the contemporary legal issues related to online personal data protection
   b. A legal approach that focuses too much on data protection law categories can have detrimental effects on protecting other fundamental rights equally involved in the digital revolution.
   c. Within the EU legal framework, personal data protection law is the primary legal reference for all the issues concerning data regulation since it can always be applied in a flexible and creative way

*Part 2 – Open questions*

1. Cause of the current COVID-19 protocols, ABC University allows its students to do the exam online. In this regard, the Dean of ABC decided to adopt new software to detect possible violations of the ethics code just by capturing the facial expression of the candidates. To take part in the online exams, students must consent to process their personal data. *If you focus on the legal basis of these processing activities, which problems could ABC University face according to the GDPR?*

2. To prevent any possible vandalism, the Museum of Beauty decided to install a new video surveillance system in all its exposition rooms. CCTV is considered a valuable solution since it allows real-time detection of any possible infraction without identifying the people involved. *If you focus on one of the fundamental principles of data protection law (according to the GDPR), what are the pros and cons of this privacy strategy?*

*Part 3 – Reading and comprehension*

*TASK: In light of what you have studied about EU data protection strategy, what is your position about the author's point of view? And, in your opinion, what is the most problematic issue of his proposal?*

* * *

**Navigating data privacy legislation in a global society**
by Daniel Barber on TechCruch.com

China, the most populous nation in the world, passed its first significant data privacy legislation in August. Moving forward, any global business or aspiring startup doing any type of trade or offering services online likely will be affected because they'll be engaging with Chinese residents covered by the Personal Information Protection Law (PIPL).

Although this seems like pretty significant news, the legislation itself is similar to the EU's General Data Protection Regulation (GDPR), which was introduced in 2016. What is shocking, however, is that companies had two years to prepare for GDPR, while PIPL goes into effect on November 1, 2021.

This leaves companies scrambling to figure out compliance. In addition, it highlights the importance and urgency of data privacy on a global scale. China marks the 17th country to establish a GDPR-like privacy law. Which global superpower is not on this list?

The United States has yet to adopt a broad-reaching, consumer-focused national data privacy law — despite multiple studies indicating that Americans want more control over their personal data online. This oversight has significant implications for the technology industry in particular.

With so much going on, it's clear that we've reached a critical juncture in the maturation of data privacy. How we proceed will affect potentially billions of consumers worldwide as well as the development of companies ranging from the smallest startups to the biggest global enterprises. This moment demands careful consideration.

As such, let's attempt to break down the present data privacy conundrum, starting first by examining how data privacy legislation is evolving in the U.S. and what this means on a broader scale, before diving into how data minimization attempts address these issues. After weighing these integral pieces of the data privacy puzzle, I will conclude by issuing a call for global data privacy standards that place people firmly in control of their data.

**Data minimization is not the only answer**

One approach being bandied about to help address data privacy involves the principle of data minimization, which allows companies to collect and retain personal information only for a specific purpose.

Basically, it's a call for companies to simply collect less data. Think marketing teams reducing their intake or establishing retention schedules to purge existing data.

This is great for some, but for others, it can be unrealistic. Even the most consumer-friendly companies are unlikely to encourage marketers to go out and collect less personal information about potential customers, and they could nearly always find a justification for grabbing data.

But, the practice, even in its purest state, could be detrimental to startups that rely on personal information and preferences to develop products and grow their businesses. Data minimization in this sense could have the unintended consequence of stifling innovation.

[...]

**A call for global data privacy standards**

It is my view that all of these complexities, fine lines and moving parts are surfacing and posing problems for companies and consumers because there is no global standard to get people on the same page. Until one exists, everything else is just a Band-Aid.

[...]

Data privacy standards would establish a baseline of fairness that spans geographic borders and works for companies at any stage. This would make it exponentially easier for companies to engage in business internationally.

Expect the existing spheres of influence to drive this change. Because there are massive, negative and costly implications on the line for any company that even hopes to go global, entities will work together to create common solutions. The momentum is there. Considering the footprint of China alone, it won't be long until other countries follow suit.

**The heart of data privacy standards**

Data privacy standards are now necessary, and the main thing to remember as they develop is that we must give people control over how companies handle their information.

Consumers deserve to know who has access to their information and why, particularly as services and applications become more connected to facilitate transactions. They should also have the right for personal data to be deleted upon request as well as to prevent companies from selling their information without permission. These are basic, universal rights; these are the things governing and supporting bodies should agree on.

Although marketers may grouse, it shouldn't just be assumed that all consumers object to sharing their information. In fact, many appreciate the customization of experiences or ease of transactions that are made possible by allowing companies to collect and retain their personal information, as noted in the examples above.

Consumer choice ultimately creates a healthier ecosystem overall and opens up new ways for companies to build trust and transparency. It will also prevent companies from perpetually scrambling to develop and manage a slew of different mandates.

I foresee a future where startups are founded as privacy first. This is even likely to become a true differentiator. But the biggest element of change will be to give consumers unquestionable control of their data, no matter where they are, or the systems that contain their personal information. Data privacy standards will protect these rights in ways that other approaches can't reasonably replicate or deploy at scale; they will eliminate confusion so that businesses can operate efficiently.

Once we are all on the same page through data privacy standardization, true progress can be made.