23 EXAMS

(This section is dedicated to the material present between the Telegram group and what I archived in MEGA regarding the course, the material and exams + mock test present)

General rules – Instructions

You will have 75 minutes to conclude your test, which is divided into two sections and totally counts 8 questions.

The first part includes multiple-choice questions. Please, consider that some of them may have more than one correct answer.

The second part is made up of open questions. You are warmly invited to answer using the maximum recommended number of words.

Every question specifies the maximum number of points recognized for each correct answer in the overall assessment of your exam.

23.1 MOCK TEST – 17 JANUARY 2024

23.1.1 Multiple choice questions (MCQ)

1. The main difference between the EU and the US approaches to the legal regime of personal data is (1 pt)
    a. That the EU treats personal data as as an aspect of individual personality, whereas the US treats data as a market
    b. That only EU protects privacy
    c. That only the US protect privacy
    d. That only the US approach leverages individual consent to protect privacy

2. Correcting illegal bias in AI (2 pts – more answers)
    a. Is always legitimate
    b. Must be done in a way that does not violate basic legal principles such as equality
    c. Is legally impossible
    d. Can be done only by amending the algorithm or the dataset for the training

3. The processing of personal data pursuant to the GDPR may be lawfully carried out (2 pts)
    a. When data subjects expressed their own consent
    b. Based on the controller's free choice
    c. When there is no consent by data subjects, but the processing is needed for protecting the data subjects' or other individuals' vital interests
    d. When there is no consent, but the processing must take place to perform a contract between the controller and any third party

4. Which of the following are legislative instruments belonging to EU primary law? (1 pt)
    a. Treaty of the European Union, Treaty on the functioning of the European Union, Case law of the European Court of Justice
    b. Treaty of the European Union, Treaty on the functioning of the European Union, Charter of fundamental rights of the European Union
    c. Charter of fundamental rights of the European Union, Regulations, Case-law of the European Court of Justice

5. Which of the following answers is correct? (1 pt) The hierarchical system of EU law is structured as such:
    a. (1) Primary Law, (2) Secondary Law, (3) International Agreements
    b. (1) Founding treaties, (2) International Agreements, (3) Secondary Law
    c. (1) Primary Law, (3) Secondary Law, (3) Member States law

23.1.2 Open questions

6. *Please identify and illustrate three legal problems posed by social credit systems in no more than 150 words. (up to 6 pts)* – 139 words below

Social Credit Systems are national credit ratings and blacklists, mainly developed by the government of China and allow for easy yet for monitoring purposes, with governments defining good/bad actions according to their citizens behaviour. Given its context, it enables widespread/effective monitoring, not based on simple data but multiple channels of information, often collecting vast amounts of personal data without proper consent, potentially infringing individuals rights of privacy.

Lack of due process is another issue. Decisions made by social credit systems can significantly impact people's lives, yet often lack transparency or mechanisms for appeal. This violates fundamental principles of due process and fairness in legal systems.

Discrimination is a third problem. The algorithms underlying social credit systems may perpetuate or exacerbate existing societal biases, leading to unfair treatment of certain groups based on characteristics like race, gender, or socioeconomic status.

7. *Please, explain the main principles for personal data processing in no more than 200 words. (up to 6 pts)* – 189 words below

The main principles for personal data processing are fundamental guidelines that ensure the ethical and lawful handling of individuals' personal information. These principles include:

- Lawfulness, fairness, and transparency: Data must be processed legally, fairly, and in a transparent manner that individuals can understand.
- Purpose limitation: Data should be collected for specified, explicit, and legitimate purposes and not further processed in incompatible ways.
- Data minimization: Only necessary data should be collected, adequate and relevant to the specified purpose.
- Accuracy: Personal data must be kept accurate and up-to-date, with inaccurate data promptly corrected or erased.
- Storage limitation: Data should be kept in a form that permits identification of individuals for no longer than necessary for the processing purposes.

Written by Gabriel R.

- Integrity and confidentiality: Appropriate security measures must be implemented to protect personal data against unauthorized access, loss, or damage.
- Accountability: The data controller is responsible for demonstrating compliance with these principles.
- Data subject rights: Individuals have rights regarding their personal data, including access, rectification, erasure, and objection to processing.

These principles aim to balance the interests of organizations processing data with the privacy rights of individuals, fostering trust and responsible data handling practices.

8. *Please, illustrate in no more than 100 words the EU personal data protection package adopted since 2016. (up to 6 pts) – 100 words exactly below*

The EU package adopted since 2016 centers on the General Data Protection Regulation (GDPR), used since 2018. This law strengthens individuals' rights and imposes obligations on organizations processing personal data.

Key elements include:

- Enhanced user rights (access, erasure, portability)
- Stricter consent requirements
- Data breach notification within 72 hours
- Appointment of Data Protection Officers
- Privacy by design and default
- Hefty fines for non-compliance (up to 4% of global turnover)

The package also includes the Law Enforcement Directive for data processing in criminal matters and the ePrivacy Regulation (still in draft) to address electronic communications privacy.

23.2 First Exam – 8 February 2024

23.2.1 Multiple choice questions (MCQ)

1. Which of the following statements is correct (2 pts)
    a. Synthetic data is protected by GDPR
    b. The GDPR does not cover the protection of synthetic data
    c. The GDPR prohibits the creation and the dissemination of synthetic data
    d. Synthetic data and anonymized data are the same notion

2. The European Data Protection Board is (1 pt):
    a. An agency of the European Commission with the aim of protecting the fundamental right to data protection
    b. An independent body gathering the national supervisory authorities of each EU Member State
    c. An institution provided for by the Treaty on the European Union

3. Which of the following statements is correct?
    a. Freedom of thought cannot be affected by AI technologies
    b. Freedom of thought is not considered as a human right in most jurisdictions
    c. Freedom of thought deserves protection only once the individual shares his thoughts with others
    d. Freedom of thought is considered as a human right in most jurisdictions but hardly protected in itself

4. The charter of fundamental rights recognizes the right to privacy and the right to data protection to:
    a. Only to individuals with EU citizenship
    b. All individuals provided that they are in the EU
    c. Only to EU companies

5. Which of the following statements is correct?
    a. EU regulations and directives must be directly applied in any of their provision in all Member States
    b. Regulations are directly applicable in all Member States as such, whereas directives need to be implemented by every Member State
    c. Directives are directly applicable in all Member States as such, whereas regulations need to be implemented by every Member State

23.2.2 Open questions

1. Please describe in no more than 250 words the 2020 european data strategy conceive by the european union (up to 6 pts) – 224 words

Skeleton of answer provided by professors in Moodle:

- *The GDPR that paved the way to the 2020 European Data Strategy*
- *Aims of the EU Data Strategy: free flow of personal data, free flow of non-personal data, single market for data*
- *EU Data Strategy Package: Data Governance Act, Digital Services Act, Digital Markets Act, Artificial Intelligence Act, Data Act (a summarized description of their contents)*

My answer/take:

The European Union's 2020 Data Strategy builds upon the foundation laid by the GDPR, aiming to create a single European data space. This strategy focuses on enabling the free flow of personal and non-personal data across the EU, fostering a single market for data respecting personal data.

Key aims include:

1. Ensuring data can move freely within the EU
2. Respecting European rules and values
3. Making high-quality data available for innovation

To achieve these goals, the EU introduced a comprehensive package of legislative initiatives:

1. Data Governance Act: Facilitates data sharing across sectors and borders, establishing data intermediaries.
2. Digital Services Act: Regulates online platforms, ensuring user safety and protecting fundamental rights.
3. Digital Markets Act: Addresses market imbalances in the digital sector, promoting fair competition.
4. Artificial Intelligence Act: Proposes rules for the development and use of AI systems, ensuring they are safe and respect EU values.
5. Data Act: Aims to make more data available for use, clarifying rules on data access and use in business-to-business and business-to-government contexts.

This strategy package seeks to position the EU as a leader in the data-driven economy while maintaining high standards of data protection and digital rights. By creating a harmonized approach to data governance and digital markets, the EU aims to foster innovation, economic growth, and societal benefits while upholding its core values.

2. *Please explain the so-called "Barbara Streisand Effect" in no more than 100 words (up to 6 pts)*

Skeleton of answer provided by professors in Moodle:

- *A brief summary of the facts of the case*
- *Description of the Effect: The protection of privacy through legal means can backfire and worsen the situation of the individual*
- *Takeaways:*
    - *The Legal protection of privacy can consist in avoiding seeking legal protection;*
    - *The legal vindication of privacy is different—and sometimes opposite—from the social enjoyment of privacy*

My answer/take:

3. *Please describe any legal provision included in EU primary law sources setting out the right to personal data protection in max 250 words – 230 words below*

Skeleton of answer provided by professors in Moodle:

- *Personal data protection in the TEU, starting from the values of the EU as protected by article 2 TEU and the protection thereof set out in article 3 TEU*
- *Personal data protection as set forth by article 16 TFEU*
- *The fundamental right to data protection in the Charter of Fundamental Rights (article 8 CFR) and possible reference to article 7 CFR on the right to privacy (and their differences)*
- *Possible limitations of fundamental rights and, specifically, of the right to data protection in light of the safeguard clause (article 52 CFR) – the balancing of conflicting rights*

My answer/take:

The right to personal data protection is enshrined in EU primary law through several key provisions (according to Article 8 CFR and part of the Nice Charter/EU Charter of Fundamental Rights in 2009):

- In the Treaty on European Union (TEU), Article 2 establishes respect for human rights as a core EU value. Article 3 further commits the EU to protect its citizens, which implicitly includes safeguarding their personal data.
- The Treaty on the Functioning of the European Union (TFEU) explicitly addresses data protection in Article 16. This article grants everyone the right to protection of their personal data and empowers the European Parliament and Council to establish rules on data processing.
- The Charter of Fundamental Rights (CFR) elevates data protection to a fundamental right in Article 8. This article guarantees the right to protection of personal data, requires fair data processing for specified purposes, and grants individuals rights to access and rectify their data. It's distinct from, yet complementary to, Article 7 CFR, which protects the right to privacy.
- Article 52 CFR allows for limitations on these rights, provided they are necessary, proportionate, and respect the essence of the rights. This enables balancing data protection with other rights or public interests when conflicts arise.

Written by Gabriel R.

Together, these provisions create a robust legal framework for personal data protection in EU primary law, reflecting its importance in the Union's legal order and values.

23.3 Second Exam – 22 February 2024

23.3.1 Multiple choice questions (MCQ)

6. Which of the following statements is correct (2 pts)
    a. Synthetic data is protected by GDPR
    b. The GDPR does not cover the protection of synthetic data
    c. The GDPR prohibits the creation and the dissemination of synthetic data
    d. Synthetic data and anonymized data are the same notion

7. The processing of personal data pursuant to the GDPR may be lawfully carried out (2 pts):
    a. When data subjects expressed their own consent
    b. Based on the controller's free choice
    c. When there is no consent by data subjects, but the processing is needed for protecting the data subjects' or other individuals' vital interests
    d. When there is no consent, but the processing must take place to perform a contract between the controller and any third party

8. The Charter of fundamental rights recognizes the right to privacy and the right to data protection to (1 pt):
    a. only to individuals with EU citizenship
    b. all individuals in the EU
    c. only to EU companies

9. When the European Court of Human Rights rules that a State has failed to protect a right of an individual (2 pts.):
    a. The Court's ruling replaces the domestic rule that is incompatible with the European Convention of Human Rights
    b. It is up to the State to remove the violation of the European Convention
    c. The individual can sue the State in the European Court of Human Rights

10. The European Data Protection Supervisor is (1 pt)
    a. A national authority supervising on data protection
    b. A supranational authority supervising on the activity of national supervisory authorities
    c. A supranational supervisor on any processing of personal data Member States citizens
    d. An independent body at the European level supervising on processing carried out by EU Institutions

23.3.2 Open questions

11. Please describe the structure of the "proportionality scrutiny" in no more than 200 words. (up to 6 pts) – *198 words below*

Skeleton of answer provided by professors in Moodle:

> *The answer should describe the three-steps or four-steps proportionality scrutiny that courts often employ to balance competing rights and interests. The sequence is extremely relevant because the scrutiny is a test: if a measure fails to pass one step, the measure is unlawful, and the scrutiny is over.*
>
> *The steps are the following:*
>
> a. *Does the measure under scrutiny pursue a legitimate goal?*
> b. *Is the measure concretely connected with the purported goal (this is the "rational connection" step—some courts omit it)?*
> c. *Is the measure necessary to pursue that goal? (This is the "least restrictive means" step)*
> d. *Are the benefits more than the sacrifices that the measure causes to the interests and rights that are involved?*

My answer/take:

The proportionality measurement has been a core problem when it comes to law because it is unknown how the scrutiny assessment can be implemented. This involves mainly four questions.

1. *Legitimate goal*: Does the measure pursue a legitimate aim? The court assesses if the purpose for limiting the right is valid and important enough to potentially justify the restriction.
2. *Lawful measure*: Is the measure compliant with privacy laws and frameworks? The court assesses if the purpose can be considered legitimate from a legal point of view and then accordingly remeasured when necessary
3. *Necessity* (least restrictive means): Is the measure necessary to achieve the goal, or are there less restrictive alternatives available? The court examines if the limitation on rights goes further than needed.
4. *Proportionality stricto sensu*: Do the benefits of the measure outweigh the costs to the affected rights and interests? This final balancing step weighs the positive outcomes against the negative impacts on fundamental rights.

This structured analysis helps ensure that any limitations on fundamental rights like data protection are justified, narrowly tailored, and balanced against other important interests or rights. It provides a framework for courts to systematically evaluate the lawfulness of measures

12. Please, explain what ‘personal data’ means according to the EU personal data protection legislation and the difference with sensitive personal data in no more than 200 words (up to 8 pts)

Skeleton of answer provided by professors in Moodle:

a. *definition of personal data according to article 4(1) of the GDPR*
b. *definition of sensitive data, even involving article 9 GDPR*
c. *differences in the processing of personal data and sensitive personal data*
d. *lawful reasons for processing personal data and sensitive personal data with or without data subjects’ consent*
e. *possible references to the origins of the definition of personal data and sensitive personal data (Convention 108, OECD Guidelines)*

My answer/take:

According to the EU's General Data Protection Regulation (GDPR), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). This includes identifiers such as names, identification numbers, location data, online identifiers, or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

'Sensitive personal data', referred to as 'special categories of personal data' in the GDPR, includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for unique identification, health data, and data concerning a person's sex life or sexual orientation.

The key difference lies in their processing requirements. While personal data can be processed under various lawful bases (consent, contract, legal obligation, vital interests, public task, legitimate interests), sensitive data has stricter processing conditions. Processing sensitive data is generally prohibited unless specific conditions are met, such as explicit consent or necessity for certain legal, medical, or public interest reasons.

These definitions have roots in earlier data protection frameworks like the Council of Europe's Convention 108 and the OECD Guidelines, which recognized the need for special protection of sensitive data.

13. Please, describe which are the main rights recognized to a data subject by the GDPR in max 250 words. (up to 8 pts) – *249 words below*

Skeleton of answer provided by professors in Moodle:

a. *Right to access*
b. *Right to data rectification*
c. *Right to data erasure – right to be forgotten*
d. *Right to processing restriction*
e. *Right to data portability*
f. *Right to limit the processing*
g. *Right to object to data processing*
h. *Right to lodge a complaint before the NSA*

My answer/take:

The General Data Protection Regulation (GDPR) recognizes several key rights for data subjects:

1. Right to access: Data subjects can request information about whether their personal data is being processed, where, and for what purpose. They are entitled to receive a copy of their data free of charge.

2. Right to data rectification: Individuals have the right to have inaccurate personal data corrected/completed if it is incomplete.

3. Right to erasure (Right to be forgotten): Data subjects can request the deletion of their personal data under certain circumstances, such as when data is no longer necessary for the original purpose.

4. Right to restrict processing: In certain situations, individuals can request the restriction of their personal data processing.

5. Right to data portability: Data subjects can request to receive their personal data in a machine-readable format and have the right to transmit it to another controller.

6. Right to object: Individuals can object to the processing of their personal data in certain circumstances, including for direct marketing purposes.

7. Rights related to automated decision making and profiling: Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.

8. Right to lodge a complaint: Data subjects can file a complaint with a supervisory authority if they believe their rights under the GDPR have been infringed.

These rights empower individuals with greater control over their personal data and how it is used by organizations.

23.4 SECOND EXAM – 22 FEBRUARY 2024

23.4.1 Multiple choice questions (MCQ)

14. What is the difference between regulations and directives in EU law? (2 pts)
    a. Regulations are immediately enforceable, while directives need domestic execution
    b. Regulations are binding, while directives are only exhortations
    c. Regulations establish rules, whereas directives introduce principles
    d. There is no difference between the two notions

15. Social Credit Systems are (1pt):
    a. Intrinsically incompatible with basic legal principles
    b. Problematic insofar as they are opaque and have wide ramifications for the legal, economic, and social life of a subject
    c. Forbidden under Chinese law
    d. Forbidden under U.S. Law

16. The European Data Protection Board is (2 pts):
    a. An institution provided for by the Treaty on the European Union
    b. An agency of the European Commission with the aim of protecting the fundamental right to data protection
    c. An independent body gathering the national supervisory authorities of each EU Member State

17. The EU Charter of fundamental rights expressly safeguards (up to 2 pts):
    a. The right of data controllers and processors to process anyone's personal data
    b. The right of individuals to personal data protection
    c. The right of individuals to private and family life
    d. The right of individuals to process any other individuals' personal data

18. Should data controllers and data processors be separate entities, the GDPR sets out that (up to 2 pts):
    a. Data controllers are totally free to indicate one or more data processors, the latter not being bound by any obligation towards data controllers
    b. Their relationships need to be regulated by specific contractual agreements or by different acts provided for by law
    c. Their mutual relationships need to be regulated only by an order of any competent National Supervisory Authority

23.4.2 Open questions

19. *Why is the notion of synthetic data relevant in the field of privacy protection? How would you define synthetic data? (up to 6 pts)*

Synthetic data is relevant in the field of privacy protection because it offers a way to maintain data utility while significantly reducing privacy risks associated with using real personal data.

It is artificially generated information that mimics the statistical properties and patterns of real data without containing any actual personal information from real individuals.

It's relevant for privacy because of many reasons:

- Data anonymization: Synthetic data provides a more robust form of anonymization compared to traditional methods, as it doesn't contain any real personal identifiers.
- Reduced re-identification risk: Since synthetic data is artificially created, it dramatically lowers the risk of re-identifying individuals, a common concern with anonymized real data.
- Compliance facilitation: Using synthetic data can help organizations comply with data protection regulations like GDPR while still enabling data-driven innovation and research.
- Data sharing and collaboration: Synthetic data allows for safer sharing of data between organizations or researchers without risking exposure of sensitive personal information.
- Testing and development: It provides a privacy-safe alternative for software testing, machine learning model development, and other data-intensive processes.
- Overcoming data scarcity: In fields where personal data is limited or highly sensitive, synthetic data can provide a viable alternative for analysis and model training.

20. *Please describe how the right to privacy evolved into the right to personal data protection in no more than 150 words (up to 6 pts.)*

The evolution from privacy to personal data protection reflects the changing nature of information in the digital age:

- Initially, privacy focused on the "right to be let alone," protecting individuals from intrusion into their personal lives. This concept, rooted in common law traditions, emphasized physical privacy and protection of reputation

- As technology advanced, the focus shifted to informational privacy. The proliferation of digital data collection and processing raised new concerns about how personal information was used and shared.

- In response, the right to personal data protection emerged, particularly in Europe. This right, enshrined in the EU Charter of Fundamental Rights (Article 8) and the GDPR, goes beyond traditional privacy. It provides individuals with specific rights over their data, such as access, rectification, and erasure.

Unlike privacy, data protection is more proactive, imposing obligations on data controllers and processors. It addresses not just confidentiality, but also fairness, transparency, and accountability in data processing. This evolution reflects the need for more comprehensive protection in our data-driven society.

Written by Gabriel R.