Module 13: Homework 13

Harsh Manishbhai Siddhapura

Vaibhavi Nitin Honagekar

Arunava Lahiri

Thembelihle Shongwe

Sai Shashank Nagavaram

Anandha Krishnan Senthooraan

Group: Class96958 4

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

November 19, 2023

1. **What is the difference between a natural person and a legal person?**

   A natural person is a biological identifiable human species, whose existence can be tracked from birth to demise. A legal person, on the other hand, exists only in paper or “legend” to fulfill certain obligations. There are no witnesses available to vouch for the existence of a legal person.

   A natural person is a unique, living human being with a biological existence that can be traced from birth to death. In contrast, a legal person is a fictional or abstract entity created to fulfill specific legal obligations or functions.

   While natural persons have tangible existence and can be identified through personal records and documentation, legal persons exist only in legal documentation and are not living entities. There are no real individuals associated with legal persons, and their existence is primarily for legal and administrative purposes.

2. **What is the difference between a controller and a processor?**

   In the data privacy space, a controller and processor are separated by the scope of responsibilities. A controller determines the purposes and means of processing PII, regardless of data source, whilst a processor uses guidelines and instructions of the controller to process PII. BOth functions can be done by a single person (legal or natural).

   In the realm of data privacy and protection, the roles of controller and processor are distinct based on their responsibilities. A controller is the entity or individual that determines the purposes and means of processing personally identifiable information (PII). They decide why and how PII is processed and are responsible for ensuring compliance with data protection regulations.

   On the other hand, a processor carries out the processing of PII on behalf of the controller, following the guidelines and instructions provided by the controller. It's worth noting that these roles can be carried out by the same entity, whether it's a legal person or a natural person, depending on the context of data processing.

3. List some of the key responsibilities of a DPO.

A DPO is an independent member of the privacy team reporting directly to senior management. In the GDPR space, a DPO ensures compliance and supports the data protection impact assessment (DPIA) process using a risk-based approach and sound record-keeping.

A Data Protection Officer (DPO) plays a crucial role in ensuring an organization's compliance with data protection regulations, particularly in the context of the General Data Protection Regulation (GDPR). Some of the key responsibilities of a DPO include:

- Acting as an independent member of the privacy team, reporting directly to senior management.
- Monitoring and ensuring compliance with data protection laws and regulations.
- Supporting the data protection impact assessment (DPIA) process by using a risk-based approach to assess data processing activities.
- Maintaining comprehensive and accurate records related to data processing activities.
- Providing guidance and advice to the organization and its employees on data protection matters.
- Serving as a point of contact for data subjects and supervisory authorities.
- Cooperating with supervisory authorities and acting as the organization's representative in data protection matters.

4. What is the difference between an article and a recital in the GDPR?

A recital is a collection of articles pertaining to the GDPR law whilst articles explain the foundations of each adopted measure and the outcomes they are meant to achieve. In the General Data Protection Regulation (GDPR), articles and recitals serve different purposes. Articles are the core components of the GDPR, outlining specific provisions, rules, and regulations.

Each article provides detailed information on the principles, rights, and obligations related to data protection. They form the actionable part of the GDPR and define what organizations and individuals must do to comply with the regulation.

On the other hand, recitals are introductory or explanatory statements that precede the articles. Recitals provide context and rationale for the articles. They explain the reasons behind the GDPR's provisions

and offer a more comprehensive understanding of the regulation's intentions. Recitals help in interpreting the articles and guide in the application of the law. While articles have legal binding, recitals are not legally binding but are essential for understanding the legislative background and purpose of the GDPR.

5. List and briefly describe the main objectives of the GDPR.

The main objectives of the GDPR are to protect the privacy and personal data of EU citizens. Each objective is summarized below, failure to adhere to all these objectives under the GDPR can attract hefty fines:

- Enable every person to have the fundamental right to the protection of their personal data
- Harmonize the protection of natural persons' fundamental rights and freedoms with regard to processing activities; and ensure that personal data can freely flow between member states. Apply the proportionality principle to weigh the right to privacy against other essential rights.
- Establish a robust and well-coordinated data protection framework in the EU, supported by strict enforcement, considering the significance of building the confidence necessary for the internal market's adoption of the digital economy.
- As much as possible, give natural persons the ability to manage their own personal data.
- Ensure that the laws protecting natural persons' fundamental rights and freedoms are applied uniformly and consistently.
- Strengthening and clarifying the duties and rights of individuals who handle and decide how to process personal data, as well as providing equal authority to monitor and enforce adherence to the regulations protecting personal data and corresponding penalties for violations across member states.
- When applying the GDPR, keep in mind the unique requirements of micro, small, and medium-sized businesses.

6. Explain the concepts of material scope and territorial scope.

Material scope is defined by the actions of a particular regulation, in the case of the GDPR, the types of procedures that must be followed when handling personal data. Material scope refers to the scope of actions and operations that fall under the purview of a specific data protection regulation, such as the General Data Protection Regulation (GDPR). It defines the types of procedures, activities, and processes that must comply with the regulation when handling personal data. In essence, material scope outlines what the regulation covers in terms of data processing. For example, the GDPR's material scope encompasses various data processing activities, including collection, storage, retrieval, use, and erasure of personal data. It sets the rules and requirements that organizations and individuals must adhere to when engaging in these data processing activities.

The material scope of a data protection regulation is not limited to specific sectors or industries but extends to any entity or individual that processes personal data. This means that businesses, government agencies, non-profit organizations, and other entities are subject to the regulation's provisions when they engage in covered data processing activities.

The territorial scope is defined by the reach of particular law or regulation. For the GDPR, the territorial scope is determined by the physical storage of EU citizens' personal data. Territorial scope, on the other hand, is defined by the geographical reach or jurisdiction of a particular data protection law or regulation. In the context of the GDPR, the territorial scope is determined by the physical location and activities related to the personal data of European Union (EU) citizens. The GDPR has an extraterritorial reach, meaning it applies not only to organizations based within the EU but also to entities outside the EU that process the personal data of EU citizens.

This means that even if an organization is physically located outside the EU, it must still comply with the GDPR if it meets these criteria. The territorial scope of the GDPR has extended its influence to cover a global audience due to its emphasis on protecting the privacy and data rights of EU citizens wherever their data is processed.

7. List and briefly describe the GDPR principles.

The principles of the GDPR are the same as it main objectives (Irvenldfdasd, 2019, *Chapter 13*):

- Fair, lawful, and transparent processing of personal data
- Personal data collected for one purpose should not be used for a new, incompatible, purpose. Further processing of personal data for archiving, scientific, historical, or statistical purposes is permitted, subject to appropriate laws and regulations.
- Data minimization: an organization should process only personal data that it actually needs to process in order to achieve its processing purposes.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- Integrity and confidentiality: technical and organizational measures must be taken to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure.
- Accountability: data controllers are obliged to demonstrate that its processing activities are compliant with the data protection principles

8. Explain the concept of fairness in the GDPR.

Fairness in the GDPR refers to collecting and processing data in the spirit of fairness to the data subjects. Processing that may cause injury to a individual or a group of individuals may be unfair, and reasonable expectations should be made to protect data subjects from possible adverse consequences of personal data processing. Fairness is a fundamental concept in the General Data Protection Regulation (GDPR) that governs the ethical and lawful treatment of personal data. It is one of the core principles that organizations, data controllers, and data processors must adhere to when collecting, processing, or handling personal data. The concept of fairness in the GDPR can be extended as follows:

- Ethical Data Treatment: Fairness in the GDPR demands that organizations and entities processing personal data do so in an ethical and morally responsible manner. This means that data should be collected and processed with respect for the rights and freedoms of the data subjects. It also implies that data should not be used in ways that could harm, discriminate against, or infringe upon the rights of individuals.

- Informed Consent: Fairness includes obtaining the informed and unambiguous consent of data subjects before collecting or processing their personal data. Data subjects should be fully aware of the purposes for which their data is being processed, and they should have the right to opt in or opt out of data processing activities. Transparency in data processing is a key aspect of fairness.

- Minimization of Data: Fairness encourages the principle of data minimization. This means that organizations should only collect and process data that is strictly necessary for the stated purposes. Unnecessary data should not be collected, ensuring that the data subjects' privacy and personal information are respected.

- Preventing Harm: Fairness also encompasses the responsibility of data controllers and processors to prevent any harm to data subjects. Data processing that may cause physical, financial, or psychological harm to individuals or groups may be considered unfair. This includes taking precautions to protect against data breaches, identity theft, or any adverse consequences of personal data processing.

- Non-Discrimination: Personal data should not be used in ways that discriminate against individuals based on their race, gender, religion, sexual orientation, or any other protected characteristics. Fairness mandates that data processing does not lead to unfair treatment or discrimination against data subjects.

9. List and briefly describe rights of data subjects enumerated in the GDPR.

The following rights exist for data subjects:

- Right to be Informed (Collection from Data Subject): This right grants data subjects the information they need when their personal data is collected directly from them. It ensures transparency about the purposes, processing methods, and rights of data subjects.
- Right to be Informed (Not Collected from Data Subject): Data subjects have the right to be informed when their personal data is obtained from other sources. This includes details about the source and the specific categories of data collected.
- Right of Access: Data subjects can request access to their personal data held by data controllers. This allows individuals to know how and why their data is being processed.
- Right to Rectification: Data subjects can request corrections to inaccurate or incomplete personal data. This ensures the accuracy of their information.
- Right to Erasure (Right to be Forgotten): Data subjects have the right to request the deletion of their personal data under specific circumstances. This includes situations where the data is no longer needed for its original purpose or when consent is withdrawn.
- Right to Restrict Processing: This right allows data subjects to limit the processing of their data, often while disputes or inaccuracies are being resolved.
- Right to Data Portability: Data subjects can request their personal data in a structured, machine-readable format. This right promotes data mobility and the ability to transfer data between services.
- Right to Object: Data subjects have the right to object to the processing of their personal data. This includes processing for direct marketing purposes or when legitimate interests are not compelling enough.
- Rights in Relation to Automated Decision Making and Profiling: Data subjects have the right to receive an explanation of automated decisions based on their data. They can request human intervention and challenge these decisions.

10. What is the difference between data protection by design and data protection by default?

In **data protection by design**, the controller should implement appropriate measures (technical and otherwise) at the design phases of processing and operation to ensure that data protection principles as outlined by GDPR are met, while **data protection by default** limits these measures to data at each specific point of processing.

Data Protection by Design: In this approach, data protection is integrated into the entire system or process's design phase. It means that from the very beginning, data controllers must consider data protection and implement necessary measures. This includes technical and organizational measures to ensure data protection principles, such as data minimization, are met throughout the lifecycle of data processing.

Data Protection by Default: This concept focuses on ensuring that, by default, only the necessary personal data for each specific purpose is processed. Data protection measures are applied to the processing at each point where data is used. It requires controllers to set their systems and processes to collect and process the least amount of data necessary for the intended purpose, minimizing the risks to data subjects.

11. What is meant in the GDPR by the term processing on a large scale?

Article 9, defined processing on a large scale as holding some of these data types: 1) patient data in the regular course of business by a hospital, 2) processing of travel data of individuals using a city's public transport system (e.g. tracking via. travel cards) and 3) processing of financial transactions.

Processing on a large scale, as defined in Article 9 of the GDPR, refers to extensive data processing activities that may involve substantial volumes of personal data. Examples include handling patient data by a hospital, processing travel data collected from a city's public transport system (e.g., tracking via travel cards), or managing large-scale financial transactions. Such processing is considered significant due to its potential impact on data subjects' privacy and requires specific safeguards and assessments.

12. Distinguish between the concepts of risk and high risk.

Recital 75 states that risk and high risk are separated by their likelihood of occurrence and severity, which are assessed during the risk assessment process using the nature, scope, context, and processing goal as a guide.

The difference between risk and high risk. Risk refers to the likelihood of an event occurring and the severity of its consequences, which are evaluated during a risk assessment. High risk implies that the probability and consequences of a data breach or privacy violation are notably elevated. The assessment considers the nature, scope, context, and purpose of data processing, helping organizations identify when certain data processing activities present high risks, necessitating more stringent protective measures and oversight.

13. List and briefly describe the key steps in carrying out a DPIA.

According to guidelines from the Information Commissioner's Office, the following steps are followed in a DPIA:

- Identifying the Need for a DPIA: The first step involves recognizing when a DPIA is required. This typically applies to processing activities that are likely to result in high risks to the rights and freedoms of data subjects. Organizations must assess whether a specific processing operation warrants a DPIA.

- Describing the Data to be Processed: A comprehensive and detailed description of the personal data to be processed is essential. This step involves specifying the types of data involved, their sources, how they will be used, and who will have access to them. Stakeholder consultation, including data subjects where appropriate, is essential for a thorough understanding.

- Determining Necessity and Proportionality: This step involves evaluating the necessity and proportionality of the DPIA. It considers the likelihood and severity of risks to data subjects. Assessors need to determine whether the intended processing is justified and whether it's

proportional to its purpose. If the risks are disproportionate to the benefits, this step can lead to reconsideration or adjustments in the processing.

- Identifying Measures to Mitigate Risks: In this phase, organizations identify and document measures to mitigate the risks identified in the assessment. This may include security safeguards, procedures, or changes in data processing practices designed to reduce or eliminate the risks to data subjects. The objective is to ensure that data processing aligns with the principles of the GDPR.

- Signing Off and Recording Outcomes: Once the DPIA is complete and all necessary adjustments and mitigations have been made, the assessment is formally signed off. The outcomes, including the risks identified, the measures taken, and any relevant decisions, are documented. This step ensures transparency and accountability, both of which are critical components of data protection compliance.

References

Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices (1st ed.)*. Pearson Education

UK Information Commissioner's Office (2023), *How do we do a DPIA?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/, Online publication

Hannabuss, S. (2010, August 17). Understanding Privacy 20103 Daniel J. Solove. Understanding Privacy. Cambridge, MA and London: Harvard University Press 2008.