Vidzemes Augstskola

Personal data protection / 2023

# EXAM in course Personal Data Protection 2023 (2022.06.16)

Student’s name, surname: Denys Shabelnyk <- PLEASE FILL IN

Duration of the exam is **3** (three) hours. The responses have to be handed in by the end of exam time in teacher’s email.

**EXAM RESPONSES SENT IN AFTER THE DEADLINE ARE NOT ACCEPTED (GRADED WITH 0 POINTS)**

During the exam students are allowed to use all available materials from the course as well as other materials they find useful. Copy of contents from outside materials is forbidden, except the cases where citations are used. Within each response % of citations shall not exceed 15% of overall response. Responses will be checked with content copyright tools.

Every question has the maximum number of points indicated possible for the response. The number of points should also serve as indication for you as to how much effort you should spend on specific question.

Please try to be specific in your responses (general or generic responses will be graded low). If you make assumptions about specific situations, please state them. Trying to lists all possible responses in order to “guess the right one” will have points deducted.

**PLEASE FOLLOW THE TIME ALLOCATED (SET REMINDER) SO NOT TO BE LATE!!!**

# Questions and responses

|  |  |
| --- | --- |
| Question | Response |
| 1. Question (*Right to restriction of processing)* 10 points  Describe the circumstances in which the "right to restriction of processing" can be exercised, situations in which such requests should be declined, and the necessary actions the Controller/Processor must take to fulfill these requests. Provide relevant examples for both scenarios. | You can use restrictions when: 1) data is corrupted;  2) data use without legal permits;  3) **Action by controller:** evaluate risk and closed access to the data;  4) **Action by processor:** accept instructions from controller and follow them |
| 1. Question (*Safeguards* )(10 points)  Identify and explain the safeguards provided in GDPR Articles for the transfer of personal data to third countries that are currently considered valid and effective for use. Provide a detailed explanation of their validity and usability for each safeguard and specify which safeguards require approval from the European Data Protection Board (EDPB), European Data Protection Authority (EDPA), or Supervisory Authorities (SAs) at different levels. | |  |  |  |  | | --- | --- | --- | --- | | Safeguard | Description | Should be approved by SA? | Should be approved by EDPB? | | Adequacy Decision | The European Commission made decision | No | No | | Derogations | Derogations are exceptions that allow the transfer of personal data to a third country without relying on adequacy decisions, SCCs, or BCRs.  Derogations do not require specific approval from the EDPB, EDPA, or SAs. | No | No | | Standard Contractual Clauses (SCCs) | Approved by European Commission | No | No | | Binding Corporate Rules (BCRs) | The EDPB's role is to provide guidance and cooperation between SAs but does not individually approve BCRs. | Yes | No | |
| 1. Question (*Processors and Controllers*) 10 points  Describe the fundamental distinctions between data processors and data controllers in general. Additionally, explain the potential differences between these roles in the event of a data breach on the processor's side, outlining the liabilities, responsibilities, and obligations of each party involved. Identify who would be liable, for what, and to whom in such a scenario. | **Data Controller:**  1) Responsible for overall compliance with data protection laws;  2) Reporting in case caught some violations;  3) Informing affected individuals about corrupted and illegal access to their data;  4) Responsible of save and protect personal data. **Data Processor:** 1) Helps controller to inform affected individuals about corrupted and illegal access to their data;  2) Implementing appropriate security measures to protect personal data;  3) Responsible for data protection in general |
| 1. Question (EU *Digital Health initatives and patients rights*) 20 points  Discuss the intersection of the EU Digital Health Initiative (specifically cross border initiatives which allow to use prescriptions, get lab results, etc across EU country borders) and the General Data Protection Regulation (GDPR), highlighting their implications for the protection of personal health data. Analyze the key principles and requirements of GDPR that are relevant to digital health initiatives. Examine the challenges and considerations associated with ensuring compliance with GDPR when implementing digital health solutions. Provide examples of specific measures and practices that organizations should adopt to adhere to GDPR while leveraging the benefits of the EU Digital Health Initiative referring to respective GDPR articles. | GDPR principles:  1) **Lawful Basis/following legal** – data health information can be processed only when it is needed and required following local and EU laws;  2) **Limited purpose** - data health information can be processed only for medical reasones;  3) **Minimum required data –** medical organizations should only collect and process the necessary health data, avoiding excessive data collection.  4) **Security and Confidentiality –** health data must be protect against illegal access and against public sharing;  5) **Data Subject Rights –** Individuals have access to their personal data and also have ability to delete some information from prescriptions and medical cards;  6) **Data Transfers –** the policy is allowed that with follow security and confidentiality principles |

**Questions below use the CASE STUDY (can be found in the end of this document).**

Please READ THE CASE STUDY BEFORE starting to answer the following questions which are in line with the Question 4 dilemma (don’t assume the HealthFirst type of scenario are the “preferred answer” for question 4.

|  |  |
| --- | --- |
| 1. Question (15 points)  Is there a need for patient additional consent in following scenario. Patient has agreed to give doctor access to his/her medical data stored in HealthFirst EHR, however doctor can see there is also some health data (heart rate, activity log) on the patients mobile device. HealthFirst mobile application can access this data (during install patient has said “yes” to allowing app to access this data.  Should patient give additional consent for this data or is the consent given before sufficient? Please state your assumptions and explain your logic referring also to the GDPR articles. | **GDPR articles:**  1) Article 6(1)(a) - Lawfulness of Processing  2) Article 7 - Conditions for Consent Additional juridical consents are not necessary.  A patient can give consent using verbal way. |
| 1. Question (15 points)  Rephrased exam question:   HealthFirst has received a request from a widow seeking access to her deceased husband's medical data stored in the HealthFirst Electronic Health Record (EHR) system. The widow wishes to verify if her husband's heart condition, which caused his death, was accurately diagnosed. As a representative of HealthFirst, describe how you would respond to this request. What information would you provide to the widow and how would you guide her on the next steps to proceed? | Personal data of deceased individuals can be subject to the General Data Protection Regulation (GDPR) in certain situations. On this case, an medical organization can provide information about her husband before a widow provide the certificate about death and marriage certificate. |
| 1. Question (15 points)  Security and Confidentiality:   a. Assess the security measures and safeguards HealthFirst should implement to protect special category personal data from unauthorized access, loss, or disclosure.  b. Discuss the challenges and considerations HealthFirst should address to ensure the confidentiality and integrity of special category personal data, considering the sensitivity and potential risks involved. | Actions:  1) personal trainings – work with medical staff about security, confidential and patients data protection;  2) min data – store and use only minimum patient’s data;  3) regular security assessments – in a part of personal trainings. Security checks should be run frequantly. |
| 1. Question (15 points)   (pretend to be an SA employee with relevant task)  HealthFirst has received a complaint from one of its Electronic Health Record (EHR) users regarding the handling of their personal data. The user alleges that HealthFirst has not adequately protected their privacy and that unauthorized access to their medical records has occurred. As a SA employee dealing with this complaint about HealthFirst, outline the steps you would take to address this complaint and investigate the alleged privacy breach. Provide a comprehensive plan that includes identifying the legal and ethical considerations, conducting an internal investigation, communicating with the affected user, and implementing measures to prevent future incidents. | As SA employee, I would follow these steps:   1. Accept evidences from patient and documented complaining from it 2. Checked internal documentations related with personal data protection 3. Run internal investigation with all medical team 4. After evidence is collected, I would assess the compliance HealthFirst with GDPR. 5. After investigation is finished, informed the patient about result. 6. Report to responsible board 7. After, I will protect my organization to avoided repeated issues. |
| 1. Question (25 points)   In light of international data transfers, discuss the significance and applicability of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) for HealthFirst's EHR.  1. SCCs:  a. Explain the purpose of SCCs and their role in facilitating international data transfers while ensuring adequate data protection.  b. Discuss the conditions under which HealthFirst would utilize SCCs to legitimize transfers of personal data from the European Union (EU) to third countries for EHR purposes.  c. Identify the entities involved and the obligations imposed by SCCs on HealthFirst and its data recipients.  2. BCRs:  a. Describe the concept of BCRs and their significance in the context of multinational organizations like HealthFirst.  b. Discuss the potential benefits and challenges of implementing BCRs for HealthFirst's EHR to achieve compliance and ensure consistent data protection across multiple jurisdictions.  c. Outline the steps HealthFirst would need to take to establish and obtain approval for BCRs from relevant supervisory authorities.  3. Comparative Analysis:  a. Compare and contrast SCCs and BCRs in terms of their applicability, legal frameworks, and implementation processes.  b. Assess the suitability of SCCs and BCRs for HealthFirst's EHR, taking into account factors such as the volume and sensitivity of personal data processed, the number of countries involved, and the organization's commitment to data protection.  4. Compliance Considerations:  a. Identify the key provisions of the General Data Protection Regulation (GDPR) related to international data transfers and their relevance to HealthFirst's EHR.  b. Discuss the role of supervisory authorities, such as Data Protection Authorities (DPAs), in overseeing and ensuring compliance with SCCs and BCRs for international data transfers.  5. Practical Implementation:  a. Provide recommendations on how HealthFirst can effectively implement SCCs or BCRs within its EHR system to comply with GDPR requirements and safeguard personal data during international transfers.  b. Discuss the importance of maintaining documentation, conducting periodic audits, and ensuring ongoing compliance with SCCs or BCRs.  In your responses, consider real-world examples, cite relevant articles and guidelines from GDPR and other applicable data protection regulations, and discuss the implications and considerations specific to HealthFirst's EHR and its international operations. |  |

# Case study

Case Study: Handling Personal Data of Special Categories under GDPR

Scenario:

You are a data protection officer for a healthcare organization named "HealthFirst." HealthFirst provides various medical services, including consultations, treatments, and medical research. As part of its operations, HealthFirst processes personal data that falls under the special categories of data as defined by the General Data Protection Regulation (GDPR). HealthFirst has multiple teams / subsidiaries with HQ in Amsterdam (Netherlands), branch office in Uruguay (IT service part) and another office in London (UK).

Technical Infrastructure of HealthFirst:

HealthFirst relies on a robust and secure technical infrastructure to support its healthcare operations and handle personal data, including special category data. The following is an overview of the key components in HealthFirst's technical infrastructure, accompanied by a component diagram:

1. Application Servers:

* HealthFirst utilizes application servers to host and run various healthcare applications, including electronic health records (EHR) systems, patient portals, and medical research platforms.
* These servers handle the processing and storage of special category personal data, ensuring accessibility and availability to authorized personnel.

2. Database Servers:

* Database servers are responsible for storing and managing the vast amounts of healthcare data, including special category personal data, collected by HealthFirst.
* These servers adhere to strict security measures, such as encryption and access controls, to protect the confidentiality and integrity of the stored data.

3. Network Infrastructure:

* HealthFirst's network infrastructure connects various components of the technical environment, enabling seamless data exchange and communication.
* Firewalls, intrusion detection and prevention systems, and other network security measures are implemented to safeguard against unauthorized access and potential threats.

4. Data Encryption Mechanisms:

* HealthFirst employs encryption mechanisms to protect the confidentiality of special category personal data during transmission and storage.
* Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols are used to encrypt data in transit, while encryption algorithms (e.g., AES) secure data at rest in databases or storage systems.

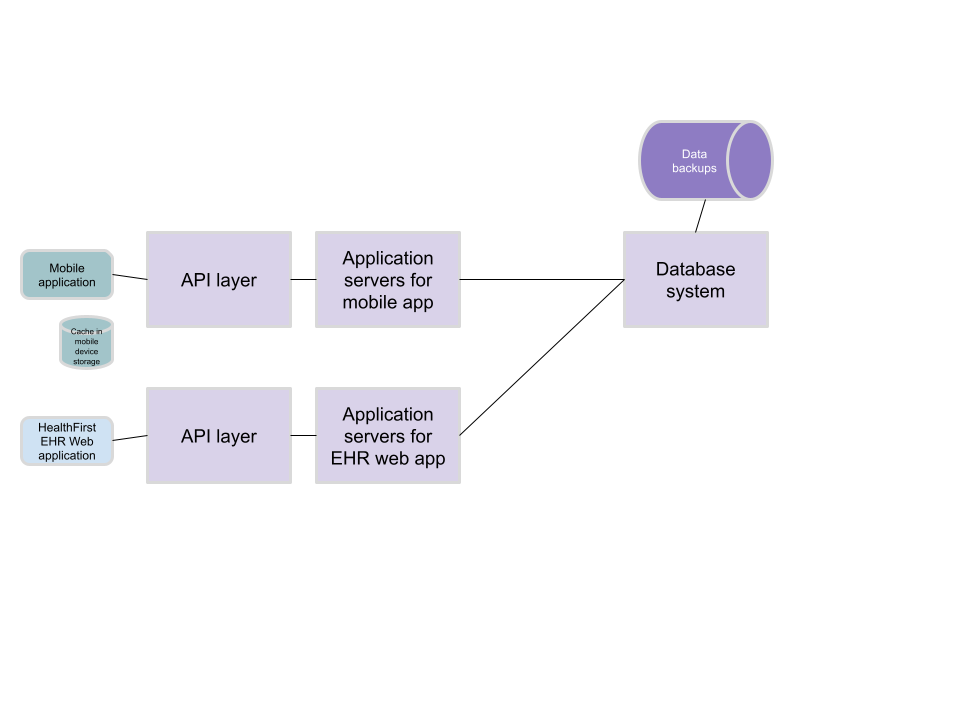
5. Authentication and Access Controls:

* HealthFirst implements robust authentication mechanisms, such as username-password combinations, multi-factor authentication (MFA), or biometric authentication, to ensure only authorized individuals can access sensitive systems and data.
* Access controls are implemented to enforce granular permissions, restricting access to special category personal data based on roles, responsibilities, and the principle of least privilege.

6. Backup and Disaster Recovery:

* HealthFirst maintains regular backups of its systems and databases to ensure data resilience and facilitate disaster recovery in case of unexpected events or data loss incidents.
* Backup data is securely stored and periodically tested to ensure its integrity and availability.

Component Diagram:



This component diagram illustrates the major components and their relationships within HealthFirst's technical infrastructure. Each component plays a vital role in supporting the secure processing, storage, and transmission of special category personal data while adhering to GDPR's requirements for data protection.