KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **GDPR**

Title : PECB Certified Data Protection Officer

Version : DEMO

1.Scenario 1:
MED is a healthcare provider located in Norway. It provides high-quality and affordable healthcare services, including disease prevention, diagnosis, and treatment. Founded in 1995, MED is one of the largest health organizations in the private sector. The company has constantly evolved in response to patients' needs.
Patients that schedule an appointment in MED's medical centers initially need to provide their personal information, including name, surname, address, phone number, and date of birth. Further checkups or admission require additional information, including previous medical history and genetic data. When providing their personal data, patients are informed that the data is used for personalizing treatments and improving communication with MED's doctors. Medical data of patients, including children, are stored in the database of MED's health information system. MED allows patients who are at least 16 years old to use the system and provide their personal information independently. For children below the age of 16, MED requires consent from the holder of parental responsibility before processing their data.
MED uses a cloud-based application that allows patients and doctors to upload and access information. Patients can save all personal medical data, including test results, doctor visits, diagnosis history, and medicine prescriptions, as well as review and track them at any time. Doctors, on the other hand, can access their patients' data through the application and can add information as needed.
Patients who decide to continue their treatment at another health institution can request MED to transfer their data. However, even if patients decide to continue their treatment elsewhere, their personal data is still used by MED. Patients' requests to stop data processing are rejected. This decision was made by MED's top management to retain the information of everyone registered in their databases.
The company also shares medical data with InsHealth, a health insurance company. MED's data helps InsHealth create health insurance plans that meet the needs of individuals and families.
MED believes that it is its responsibility to ensure the security and accuracy of patients' personal data. Based on the identified risks associated with data processing activities, MED has implemented appropriate security measures to ensure that data is securely stored and processed.
Since personal data of patients is stored and transmitted over the internet, MED uses encryption to avoid unauthorized processing, accidental loss, or destruction of data. The company has established a security policy to define the levels of protection required for each type of information and processing activity. MED has communicated the policy and other procedures to personnel and provided customized training to ensure proper handling of data processing.
Question:
If a patient requests MED to permanently erase their data, MED should:
A. Reject the request since the medical history of patients cannot be permanently erased.
B. Erase the personal data if it is no longer needed for its original purpose.
C. Erase the personal data only if required to comply with a legal obligation.
D. Refuse the request because medical data must be retained indefinitely for future reference.
Answer: B
Explanation:
Under Article 17 of the General Data Protection Regulation (GDPR), also known as the "Right to be Forgotten," data subjects have the right to request the erasure of their personal data when:
The data is no longer necessary for the purpose for which it was collected.
The data subject withdraws consent (where processing was based on consent).
The data was processed unlawfully.

In this scenario, if the data is no longer necessary for the original purpose (e.g., if the patient has completed their treatment and there are no legal retention obligations), MED should erase the data. However, there are exceptions under GDPR, such as legal retention requirements for medical records under national healthcare regulations.
Rejecting the request outright (Option A) is incorrect because GDPR requires controllers to assess whether retention is still necessary. Similarly, Option C is too restrictive because GDPR allows deletion even if no legal obligation mandates it.
Option D is incorrect because indefinite retention is not permitted unless a valid justification exists.
Reference: GDPR Article 17 (Right to Erasure)
Recital 65 (Clarification on when personal data can be erased)
Article 5(1)(e) (Storage limitation principle)

2.Scenario 1:
MED is a healthcare provider located in Norway. It provides high-quality and affordable healthcare services, including disease prevention, diagnosis, and treatment. Founded in 1995, MED is one of the largest health organizations in the private sector. The company has constantly evolved in response to patients' needs.
Patients that schedule an appointment in MED's medical centers initially need to provide their personal information, including name, surname, address, phone number, and date of birth. Further checkups or admission require additional information, including previous medical history and genetic data. When providing their personal data, patients are informed that the data is used for personalizing treatments and improving communication with MED's doctors. Medical data of patients, including children, are stored in the database of MED's health information system. MED allows patients who
are at least 16 years old to use the system and provide their personal information independently. For children below the age of 16, MED requires consent from the holder of parental responsibility before processing their data.
MED uses a cloud-based application that allows patients and doctors to upload and access information. Patients can save all personal medical data, including test results, doctor visits, diagnosis history, and medicine prescriptions, as well as review and track them at any time. Doctors, on the other hand, can access their patients' data through the application and can add information as needed.
Patients who decide to continue their treatment at another health institution can request MED to transfer their data. However, even if patients decide to continue their treatment elsewhere, their personal data is still used by MED. Patients' requests to stop data processing are rejected. This decision was made by MED's top management to retain the information of everyone registered in their databases.
The company also shares medical data with InsHealth, a health insurance company. MED's data helps InsHealth create health insurance plans that meet the needs of individuals and families.
MED believes that it is its responsibility to ensure the security and accuracy of patients' personal data. Based on the identified risks associated with data processing activities, MED has implemented appropriate security measures to ensure that data is securely stored and processed.
Since personal data of patients is stored and transmitted over the internet, MED uses encryption to avoid unauthorized processing, accidental loss, or destruction of data. The company has established a security policy to define the levels of protection required for each type of information and processing activity. MED has communicated the policy and other procedures to personnel and provided customized training to ensure proper handling of data processing.

Question:
Based on scenario 1, is the processing of children's personal data performed by MED in compliance with GDPR?
A. No, the processing of personal data of children below the age of 16 years is not in compliance with the GDPR, even if parental consent is provided.
B. Yes, the processing of children’s personal data below the age of 16 years with parental consent is in compliance with GDPR.
C. No, MED must obtain explicit consent from the child, regardless of parental consent, for the processing to be in compliance with GDPR.
D. Yes, as long as the processing is conducted with industry-standard encryption.
Answer: B
Explanation:
Under Article 8 of the GDPR, the processing of personal data of children under 16 years is only lawful if parental or guardian consent is obtained. However, Member States can lower the age limit to 13 years if they choose.
In this scenario, MED requires parental consent for children below 16 years, which aligns with GDPR requirements. Therefore, Option B is correct.
Option A is incorrect because GDPR allows parental consent.
Option C is incorrect because GDPR does not require explicit consent from the child when parental consent is given.
Option D is incorrect because encryption alone does not determine compliance.
Reference: GDPR Article 8 (Conditions for children's consent)
Recital 38 (Protection of children's data)

3.Scenario 1:
MED is a healthcare provider located in Norway. It provides high-quality and affordable healthcare services, including disease prevention, diagnosis, and treatment. Founded in 1995, MED is one of the largest health organizations in the private sector. The company has constantly evolved in response to patients' needs.
Patients that schedule an appointment in MED's medical centers initially need to provide their personal information, including name, surname, address, phone number, and date of birth. Further checkups or admission require additional information, including previous medical history and genetic data. When providing their personal data, patients are informed that the data is used for personalizing treatments and improving communication with MED's doctors. Medical data of patients, including children, are stored in the database of MED's health information system. MED allows patients who are at least 16 years old to use the system and provide their personal information independently. For children below the age of 16, MED requires consent from the holder of parental responsibility before processing their data.
MED uses a cloud-based application that allows patients and doctors to upload and access information. Patients can save all personal medical data, including test results, doctor visits, diagnosis history, and medicine prescriptions, as well as review and track them at any time. Doctors, on the other hand, can access their patients' data through the application and can add information as needed.
Patients who decide to continue their treatment at another health institution can request MED to transfer their data. However, even if patients decide to continue their treatment elsewhere, their personal data is still used by MED. Patients’ requests to stop data processing are rejected. This decision was made by

MED’s top management to retain the information of everyone registered in their databases.
The company also shares medical data with InsHealth, a health insurance company. MED's data helps InsHealth create health insurance plans that meet the needs of individuals and families.
MED believes that it is its responsibility to ensure the security and accuracy of patients’ personal data. Based on the identified risks associated with data processing activities, MED has implemented appropriate security measures to ensure that data is securely stored and processed.
Since personal data of patients is stored and transmitted over the internet, MED uses encryption to avoid unauthorized processing, accidental loss, or destruction of data. The company has established a security policy to define the levels of protection required for each type of information and processing activity. MED has communicated the policy and other procedures to personnel and provided customized training to ensure proper handling of data processing.
Question:
Considering the nature of data processing activities described in scenario 1, is GDPR applicable to MED?
A. Yes, GDPR is applicable to MED due to its processing activities involving personal information.
B. Yes, MED’s use of cloud-based software to store and process health-related information necessitates compliance with GDPR’s data protection requirements.
C. No, MED’s activities include healthcare services within one of the four EFTA states, which do not fall under the scope of GDPR.
D. No, because MED operates only in Norway, and GDPR does not apply to domestic processing.
Answer: A
Explanation:
GDPR applies to any organization that processes personal data of individuals within the European Economic Area (EEA), regardless of the organization's location. Since MED is based in Norway, which is an EEA country, and processes personal health data, it must comply with GDPR.
Option A is correct because GDPR applies to all controllers and processors within the EEA.
Option B is misleading because while cloud-based software is relevant, the primary reason GDPR applies is MED’s processing of personal data.
Option C is incorrect because EFTA states (including Norway) are subject to GDPR.
Option D is incorrect because GDPR applies to all personal data processing in the EEA.
Reference: GDPR Article 3 (Territorial Scope)
Recital 22 (GDPR applies to EEA countries)

4.Scenario 1:
MED is a healthcare provider located in Norway. It provides high-quality and affordable healthcare services, including disease prevention, diagnosis, and treatment. Founded in 1995, MED is one of the largest health organizations in the private sector. The company has constantly evolved in response to patients' needs.
Patients that schedule an appointment in MED's medical centers initially need to provide their personal information, including name, surname, address, phone number, and date of birth. Further checkups or admission require additional information, including previous medical history and genetic data. When providing their personal data, patients are informed that the data is used for personalizing treatments and improving communication with MED's doctors. Medical data of patients, including children, are stored in the database of MED's health information system. MED allows patients who are at least 16

years old to use the system and provide their personal information independently. For children below the age of 16, MED requires consent from the holder of parental responsibility before processing their data.
MED uses a cloud-based application that allows patients and doctors to upload and access information. Patients can save all personal medical data, including test results, doctor visits, diagnosis history, and medicine prescriptions, as well as review and track them at any time. Doctors, on the other hand, can access their patients' data through the application and can add information as needed.
Patients who decide to continue their treatment at another health institution can request MED to transfer their data. However, even if patients decide to continue their treatment elsewhere, their personal data is still used by MED. Patients' requests to stop data processing are rejected. This decision was made by MED's top management to retain the information of everyone registered in their databases.
The company also shares medical data with InsHealth, a health insurance company. MED's data helps InsHealth create health insurance plans that meet the needs of individuals and families.
MED believes that it is its responsibility to ensure the security and accuracy of patients' personal data. Based on the identified risks associated with data processing activities, MED has implemented appropriate security measures to ensure that data is securely stored and processed.
Since personal data of patients is stored and transmitted over the internet, MED uses encryption to avoid unauthorized processing, accidental loss, or destruction of data. The company has established a security policy to define the levels of protection required for each type of information and processing activity. MED has communicated the policy and other procedures to personnel and provided customized training to ensure proper handling of data processing.
Question:
Based on scenario 1, MED shares patients' personal data with a health insurance company.
Does MED comply with the purpose limitation principle?
A. Yes, personal data may be used for purposes in the public interest or statistical purposes in accordance with Article 89 of GDPR.
B. Yes, using personal data for creating health insurance plans is within the scope of the data collection purpose.
C. No, personal data should be collected for specified, explicit, and legitimate purposes in accordance with Article 5 of GDPR.
D. Yes, as long as the data is encrypted before sharing.
Answer: C
Explanation:
Under Article 5(1)(b) of GDPR, personal data must be collected for specific, explicit, and legitimate purposes and cannot be further processed in a manner incompatible with those purposes. Sharing medical data with an insurance company is a separate purpose and requires explicit consent or another lawful basis.
Reference: GDPR Article 5(1)(b) (Purpose limitation)

5.Scenario 1:
MED is a healthcare provider located in Norway. It provides high-quality and affordable healthcare services, including disease prevention, diagnosis, and treatment. Founded in 1995, MED is one of the largest health organizations in the private sector. The company has constantly evolved in response to patients' needs.
Patients that schedule an appointment in MED's medical centers initially need to provide their personal

information, including name, surname, address, phone number, and date of birth. Further checkups or admission require additional information, including previous medical history and genetic data. When providing their personal data, patients are informed that the data is used for personalizing treatments and improving communication with MED's doctors. Medical data of patients, including children, are stored in the database of MED's health information system. MED allows patients who are at least 16 years old to use the system and provide their personal information independently. For children below the age of 16, MED requires consent from the holder of parental responsibility before processing their data.
MED uses a cloud-based application that allows patients and doctors to upload and access information. Patients can save all personal medical data, including test results, doctor visits, diagnosis history, and medicine prescriptions, as well as review and track them at any time. Doctors, on the other hand, can access their patients' data through the application and can add information as needed.
Patients who decide to continue their treatment at another health institution can request MED to transfer their data. However, even if patients decide to continue their treatment elsewhere, their personal data is still used by MED. Patients' requests to stop data processing are rejected. This decision was made by MED's top management to retain the information of everyone registered in their databases.
The company also shares medical data with InsHealth, a health insurance company. MED's data helps InsHealth create health insurance plans that meet the needs of individuals and families.
MED believes that it is its responsibility to ensure the security and accuracy of patients' personal data. Based on the identified risks associated with data processing activities, MED has implemented appropriate security measures to ensure that data is securely stored and processed.
Since personal data of patients is stored and transmitted over the internet, MED uses encryption to avoid unauthorized processing, accidental loss, or destruction of data. The company has established a security policy to define the levels of protection required for each type of information and processing activity. MED has communicated the policy and other procedures to personnel and provided customized training to ensure proper handling of data processing.
Question:
Based on scenario 1, which data subject right is NOT guaranteed by MED?
A. Right to be informed
B. Right to restriction of processing
C. Right to data portability
D. Right to rectification
Answer: B
Explanation:
Under Article 18 of GDPR, the right to restriction of processing allows data subjects to request that processing of their personal data be limited under certain conditions, such as when accuracy is contested or processing is unlawful but the data subject opposes erasure.
From the scenario, MED does not provide the option to restrict processing, as patients who request to stop processing are denied. This makes Option B correct.
Option A is incorrect because MED does inform patients about data collection purposes.
Option C is incorrect because medical data could be transferred to other institutions.
Option D is incorrect because rectification of inaccurate data is a standard obligation.
Reference: GDPR Article 18 (Right to restriction of processing)
GDPR Article 12 (Transparent communication with data subjects)