Question #1 *Topic 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, as a response to patients' needs.

Patients that schedule an appointment in MED's medical centers need to initially provide their personal information, including name and surname, address, phone number, and date of birth. Further checkup or admission requires extra information, including previous medical history and genetic data. When providing the personal data, patients are informed that the data is used for personalizing their treatments and improving the communication between them and 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 prescription, 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 the treatment in another health institution can request by MED to transfer their data. Even if patients decide to continue their treatment in other health institutions, their personal data is still used by MED and patients' requests to stop data processing are rejected. This has been decided from MED's top management in order to save the information of everyone who gets registered in their databases. The company 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 the patients' personal data. Thus, based on the identified risks presented by 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 information and processing activity. MED has communicated the policy and other procedures to the personnel and provided customized training to all personnel to ensure that it is able to use MED's systems needed for data processing.

Based on this scenario, answer the following question:

If a patient requests MED to permanently erase their data, MED should:

A. Reject the request since 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 in case it is needed to comply with a legal obligation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Based on scenario 1, is the processing of children's personal data performed by MED in compliance with the 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 the GDPR

C. No, MED must obtain explicit consent from the child, regardless of parental consent, for the processing to be in compliance with the GDPR

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Considering the nature of data processing activities described in scenario 1, is GDPR applicable to MED?

A. Yes, the GDPR is applicable to MED due to its processing activities involving personal information

B. Yes, MED uses cloud-based software to store and process health-related information necessitates compliance with the GDFR'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 the GDPR

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Based on scenario 1, MED shares their 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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Scenario 2: Soyled is a retail company that sells a wide range of electronic products from top European brands. It primarily sells its products in its online platforms (which include customer reviews and ratings), despite using physical stores since 2015. Soyled's website and mobile app are used by millions of customers. Soyled has employed various solutions to create a customer-focused ecosystem and facilitate growth.
Soyled uses customer relationship management (CRM) software to analyze user data and administer the interaction with customers. The software allows the company to store customer information, identify sales opportunities, and manage marketing campaigns. It automatically obtains information about each user's IP address and web browser cookies. Soyled also uses the software to collect behavioral data, such as users' repeated actions and mouse movement information.
Customers must create an account to buy from Soyled's online platforms. To do so, they fill out a standard sign-up form of three mandatory boxes (name, surname, email address) and a non-mandatory one (phone number).
When the user clicks the email address box, a pop-up message appears as follows:
"Soyled needs your email address to grant you access to your account and contact you about any changes related to your account and our website. For further information, please read our privacy policy."
When the user clicks the phone number box, the following message appears:
"Soyled may use your phone number to provide text updates on the order status. The phone number may also be used by the shipping courier."
Once the personal data is provided, customers create a username and password, which are used to access Soyled's website or app. When customers want to make a purchase, they are also required to provide their bank account details.
When the user finally creates the account, the following message appears:
"Soyled collects only the personal data it needs for the following purposes: processing orders, managing accounts, and personalizing customers' experience. The collected data is shared with our network and used for marketing purposes."
Soyled uses personal data to promote sales and its brand. If a user decides to close the account, the personal data is still used for marketing purposes only. Last month, the company received an email from John, a customer, claiming that his personal data was being used for purposes other than those specified by the company. According to the email, Soyled was using the data for direct marketing purposes. John requested details on how his personal data was collected, stored, and processed.
Based on this scenario, answer the following question:
When completing the sign-up form, the user gets a notification about the purpose for which the company collects their email address. Is Soyled required by the GDPR to do so?

A. Yes, users must be informed of the purpose of collecting their personal data

B. No, Soyled should provide this information only when requested by users

C. No, Soyled only needs to inform users about how their data is collected, stored, or processed

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

The GDPR indicates that the processing of personal data should be based on a legal contract with the data subject. Based on scenario 2, has Soyled fulfilled this requirement?

A. Yes, data subjects are informed about the purpose of collecting the email address and phone number before the data is collected

B. Yes, once the account is created, Soyled informs its customers that their personal data will be shared with the network

C. No, data subjects are informed that the personal data will be shared with Soyled's network only after the personal data is collected

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Based on scenario 2, Soyled only has three mandatory fields in its sign-up form. On which principle is this decision based?

A. Lawfulness, fairness, and transparency

B. Purpose limitation

C. Data minimization

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Based on scenario 2, is John's request eligible under the GDPR?

A. No, data subjects can request access to how their data is being collected, but not the details about its processing or storage

B. No, data subjects are not eligible to request details on the collection, storage, or processing of their personal data

C. Yes, data subjects have the right to request details on how their personal data is collected, stored, and processed

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Based on scenario 2, Soyled's customers are required to provide their bank account details to buy a product. According to the GDPR, is this data processing lawful?

A. Yes, because the processing is necessary for the fulfillment of the purchase agreement

B. Yes, because Soyled has a privacy policy in place which ensures the protection of personal data

C. No, sensitive data, such as bank account details, should only be processed by official authorities

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Scenario 3: COR Bank is an international banking group that operates in 31 countries. It was formed as the merger of two well-known investment banks in Germany. Their two main fields of business are retail and investment banking. COR Bank provides innovative solutions for services such as payments, cash management, savings, protection insurance, and real-estate services.
COR Bank has a large number of clients and transactions. Therefore, they process large information, including clients' personal data. Some of the data from the application processes of COR Bank, including archived data, is operated by Tibko, an IT services company located in Canada. To ensure compliance with the GDPR, COR Bank and Tibko have reached a data processing agreement. Based on the agreement, the purpose and conditions of data processing are determined by COR Bank. However, Tibko is allowed to make technical decisions for storing the data based on its own expertise.
COR Bank aims to remain a trustworthy bank and a long-term partner for its clients. Therefore, they devote special attention to legal compliance. They started the implementation process of a GDPR compliance program in 2018. The first step was to analyze the existing resources and procedures. Lisa was appointed as the data protection officer (DPO). Being the information security manager of COR Bank for many years, Lisa had knowledge of the organization's core activities. She was previously involved in most of the processes related to information systems management and data protection.
Lisa played a key role in achieving compliance to the GDPR by advising the company regarding data protection obligations and creating a data protection strategy. After obtaining evidence of the existing data protection policy, Lisa proposed to adapt the policy to specific requirements of GDPR. Then, Lisa implemented the updates of the policy within COR Bank.
To ensure consistency between processes of different departments within the organization, Lisa has constantly communicated with all heads of departments. As the DPO, she had access to several departments, including HR and Accounting Department. This assured the organization that there was a continuous cooperation between them.
The activities of some departments within COR Bank are closely related to data protection. Therefore, considering their expertise, Lisa was advised from the top management to take orders from the heads of those departments when taking decisions related to their field.
Based on this scenario, answer the following question:
Considering the GDPR's territorial scope and the details of the data processing arrangement between COR Bank and Tibko, which of the following best describes Tibko's obligations under the GDPR?

A. Tibko's compliance with the GDPR is limited to implementing technical safeguards for data storage, as stipulated by the data processing agreement with COR Bank

B. Tibko must adhere to all GDPR provisions independently, including determining the purpose of processing personal data, as a processor acting under COR Bank's authority

C. Tibko is required to comply with the GDPR because it processes personal data on behalf of COR Bank, and COR Bank determines the purpose of processing under their agreement

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

According to scenario 3, Lisa was appointed as the data protection officer. Is this action in compliance with GDPR?

A. Yes, the DPO may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract

B. Yes, the DPO must be a staff member of the controller or processor in all cases when the processing includes special categories of data

C. No, an external DPO must be contracted in cases when the personal data is collected or processed by an organization that is not established in the European Union

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Lisa implemented the updates of the data protection policy. Is Lisa responsible for this according to GDPR? Refer to scenario 3.

A. No, the DPO is only responsible for proposing changes and obtaining evidence regarding specific GDPR requirements included in the data protection policy

B. No, the DPO is responsible for monitoring compliance with GDPR but not for implementing the GDPR compliance policies

C. Yes, the DPO is responsible for the implementation of the GDPR policies, procedures, and processes, as well as ensuring compliance with GDPR

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

According to scenario 3, Tebko stores archived data on behalf of COR Bank. This means that they are a:

A. Data controller, since they control some of the data from the application processes of COR Bank

B. Data processor, since they store COR Bank's data based on the purpose and conditions defined by COR Bank

C. Joint controller with COR Bank, since they archive COR Bank's data and take technical decisions regarding data protection

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Based on scenario 3, Lisa was advised to take orders from the heads of other departments. Is this acceptable?

A. Yes, only heads of departments within a financial institution are allowed to give orders to the DPO

B. Yes, the DPO shall take instructions and tasks from employee members if required by the organization

C. No, the organization should not influence, nor put pressure to the DPO for any decision taken

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

Scenario 4: Berc is a pharmaceutical company headquartered in Paris, France, known for developing inexpensive improved healthcare products. They want to expand to developing life-saving treatments. Berc has been engaged in many medical researches and clinical trials over the years. These projects required the processing of large amounts of data, including personal information. Since 2019, Berc has pursued GDPR compliance to regulate data processing activities and ensure data protection.

Berc aims to positively impact human health through the use of technology and the power of collaboration. They recently have created an innovative solution in participation with Unty, a pharmaceutical company located in Switzerland. They want to enable patients to identify signs of strokes or other health-related issues themselves. They wanted to create a medical wrist device that continuously monitors patients' heart rate and notifies them about irregular heartbeats.

The first step of the project was to collect information from individuals aged between 50 and 65. The purpose and means of processing were determined by both companies. The information collected included age, sex, ethnicity, medical history, and current medical status. Other information included names, dates of birth, and contact details. However, the individuals, who were mostly Berc's and Unty's customers, were not aware that there was an arrangement between Berc and Unty and that both companies have access to their personal data and share it between them.

Berc outsourced the marketing of their new product to an international marketing company located in a country that had not adopted the adequacy decision from the EU commission. However, since they offered a good marketing campaign, following the DPO's advice, Berc contracted it. The marketing capaign included advertisement through telephone, emails, and social media. Berc requested that Berc's and Unty's clients be first informed about the product. They shared the contact details of clients with the marketing company.

Based on this scenario, answer the following question:

Unty is a pharmaceutical company located in Switzerland. Is the transfer of data from Berc to Unty in compliance with the GDPR?

A. Yes, Berc can transfer data to Unty because Switzerland provides a level of data protection that is "essentially equivalent" to that of the EU

B. Yes, Berc can transfer data to Unty because they collected data for the same purpose

C. No, Berc cannot transfer data to a company located in Switzerland unless authorization from the supervisory authority in France is obtained

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Based on scenario 4, Berc followed the DPO's advice for outsourcing an international marketing company in the absence of an adequacy decision. Is the DPO responsible for evaluating this case?

A. Yes, the DPO should evaluate the cases when the adequacy decision is absent

B. Yes, the DPO takes the decision of transferring personal data to an international company in the absence of an adequacy decision

C. No, the controller or processor should evaluate the cases when the adequacy decision is absent

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Based on scenario 4, Berc shared personal information of its clients with an international marketing company even though an adequacy decision was absent. Which of the following can be a valid reason to do so?

A. The transfer of data does not depend on the adoption of the adequacy decision by the country in which the company is located

B. Authorization for data transfer from Berc's chief information security officer is obtained

C. The controller or processor provides appropriate levels of data protection

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

According to scenario 4, individuals from whom the health data was collected were not informed about the arrangement between Berc and Unty. Which option below is correct in this case?

A. The arrangement and roles and responsibilities of Berc and Unty should be available to individuals

B. Berc and Unty have determined the purpose and means of processing, so they can decide if they want to inform individuals or not

C. The data processing means, purpose, or other arrangements between Berc and Unty is considered confidential information which cannot be fully available to individuals

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Based on scenario 4, to which of the companies can the data subject exercise their rights under GDPR?

A. Data subjects may exercise their rights under the GDPR against both Berc and Unty, regardless of the terms of the arrangement

B. Data subjects may exercise their rights under the GDPR against only one of the controllers, as specified in the arrangement between the two companies

C. Data subjects may exercise their rights under the GDPR against Berc only because it decided to implement GDPR for data processing activities

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Scenario 5: Recpond is a German employment recruiting company. Their services are delivered globally and include consulting and staffing solutions. In the beginning, Recpond provided its services through an office in Germany. Today, they have grown to become one of the largest recruiting agencies, providing employment to more than 500,000 people around the world.
Recpond receives most applications through its website. Job searchers are required to provide the job title and location. Then, a list of job opportunities is provided. When a job position is selected, candidates are required to provide their contact details and professional work experience records. During the process, they are informed that the information will be used only for the purposes and period determined by Recpond.
Recpond's experts analyze candidates' profiles and applications and choose the candidates that are suitable for the job position. The list of the selected candidates is then delivered to Recpond's clients, who proceed with the recruitment process. Files of candidates that are not selected are stored in Recpond's databases, including the personal data of candidates who withdraw the consent on which the processing was based.
When the GDPR came into force, the company was unprepared. The top management appointed a DPO and consulted him for all data protection issues. The DPO, on the other hand, reported the progress of all data protection activities to the top management. Considering the level of sensitivity of the personal data processed by Recpond, the DPO did not have direct access to the personal data of all clients, unless the top management deemed it necessary.
The DPO planned the GDPR implementation by initially analyzing the applicable GDPR requirements. Recpond, on the other hand, initiated a risk assessment to understand the risks associated with processing operations. The risk assessment was conducted based on common risks that employment recruiting companies face.
After analyzing different risk scenarios, the level of risk was determined and evaluated. The results were presented to the DPO, who then decided to analyze only the risks that have a greater impact on the company. The DPO concluded that the cost required for treating most of the identified risks was higher than simply accepting them. Based on this analysis, the DPO decided to accept the actual level of the identified risks.
After reviewing policies and procedures of the company, Recpond established a new data protection policy. As proposed by the DPO, the information security policy was also updated. These changes were then communicated to all employees of Recpond.
Based on this scenario, answer the following question:
Recpond stores files of candidates that are not selected in its databases even though they withdraw the consent for data processing. Is this acceptable?

A. No, the GDPR requires the controller to erase personal data if the data subject withdraws their consent for data processing

B. Yes, the GDPR only requires the controller to stop processing the data when consent is withdrawn, but does not require its deletion

C. Yes, the GDPR allows personal data to be processed even after consent is withdrawn so that organizations can use the data for future recruitment opportunities

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Based on scenario 5, the DPO reports directly to Recpond's top management. Is this in alignment with GDPR requirements?

A. Yes, Article 38 of the GDPR requires that the DPO reports directly to the highest management level of the controller

B. No, Article 38 of the GDPR requires that the DPO reports directly to the supervisory authority to ensure independence in performing the tasks

C. Yes, based on GDPR, the controller may choose any reporting structure for the DPO, including top and middle management

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

According to scenario 5, the DPO decided to accept most of the identified risks related to data processing. Is this acceptable?

A. Yes, the cost required for implementing appropriate risk controls was higher than simply deciding to accept them

B. No, the DPO should have been involved in all risk management activities in order to select an appropriate risk treatment option

C. No, the role of the DPO in risk management is to help the company select the risk treatment option, not take decisions in regard to risk treatment

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Based on scenario 5, Recpond established and communicated the data protection policy to all employees. What should the DPO ensure in this regard?

A. That all policies within Recpond are reviewed and updated by the DPO

B. That the employee awareness on the data protection policy is monitored

C. That the updates of the data protection policy are communicated to all employees through an official letter

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

According to scenario 5, what should Recpond have considered when assessing the risks related to processing operations?

A. Risks related to processing operations should be identified based on threats and vulnerabilities that the company faces

B. Risks related to processing operations should be analyzed using a quantitative approach, since risk scenarios make the risk evaluation process difficult

C. Risks related to processing operations should be assessed based on the risk-based approach adopted by the DPO

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Which statement regarding the material scope of the GDPR is incorrect?

A. The GDPR applies to the processing of personal data wholly or partly by automated means

B. The GDPR applies to the processing of personal data in the course of an activity which falls outside the scope of Union law

C. The GDPR does not apply to the processing of personal data by Member States when carrying out activities that fall within the scope of the Treaty on European Union (TEU)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

A patient gave consent for the use of their laboratory tests to defend a clinical laboratory against a lawsuit. As a result, the court required to collect and process the patient's health data and such information was revealed in court. Is this compliant with the GDPR lawfulness of processing requirement?

A. Yes, because the data subject has consented on the processing of health data and the GDPR allows the processing of special categories of personal data where it is necessary for the establishment, exercise, or defense of legal claims

B. Yes, but only if the processing of special categories of personal data is controlled by a public health institution and the data subject has consented on the processing of this type of data

C. No, although the data subject has consented on the processing of health data, the GDPR does not allow the disclosure of special categories of personal data by health institutions

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

You work in a company that provides training services. One of the clients makes an online request for access regarding the categories of recipients to whom personal data will be disclosed. What actions would you take to be compliant with the GDPR?

A. Obtain an authorization from the recipients to whom personal data will be disclosed

B. Verify the identity of the client by sending login data to their mailing address

C. Inform the client that access to this type of information is not allowed, since it may result in a high risk to the rights and freedoms of recipients

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Which of the following options is the DPO's responsibility when processing of personal data related to criminal convictions is carried by official authority?

A. Determining the location where sensitive data may be processing

B. Assessing the necessity of knowing a data subject's identity

C. Ensuring compliance with any legal requirements of Member States

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

BookSt is an online book shop that collects personal data prior to selling its product. Sarah signed up for an account on their website, providing personal data, such as her name, email address, and password. To purchase a book, Sarah was required to provide her shipping address and payment information which is needed to calculate shipping costs and complete the transaction. Does the company have a legal basis for processing Sarah's data?

A. No, the processing is not legally justified if it is only for sales purposes

B. Yes, the processing is necessary for the performance of a contract to which the data subject is a party of

C. No, the processing is legally justified only if it is necessary to protect the vital interests of the data subject

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

To evaluate the effectiveness of communication, the DPO of Company ABC evaluated the accuracy and relevance of the information provided to the company's customers regarding personal data processing. Is this a good practice?

A. Yes, when evaluating the effectiveness of communication, the DPO should consider the accuracy and relevance of the information provided to concerned parties

B. No, the effectiveness of communication cannot be evaluated through the evaluation of the accuracy and relevance of information provided to the company's customers

C. No, the DPO is not responsible for evaluating the effectiveness of communication with company's customers

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

Based on Article 58 of the GDPR, what powers must the supervisory authority have?

A. To appoint a single DPO in a group of undertakings

B. To obtain access to any premises of the controller and the processor, including data processing equipment

C. To assign the tasks of the controller or the processor and to monitor their implementation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

Organization XYZ has just appointed a DPO. As such, XYZ needs to establish the DPO's role in the employment contract. Which of the statements below holds true?

A. The DPO acts as a contact point between the supervisory authorities and the controller

B. The DPO acts as a contact point between the controller and the processor

C. The DPO act as a contact point between the organization's top management and employees

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

What is the role of the European Data Protection Board (EDPB)?

A. To supervise and monitor the application of the GDPR within the EU

B. To advise the European Commission regarding the issues related to data protection in the EU

C. To negotiate and adopt EU laws as per the proposals from the EU Commission

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

All the statements below regarding the lawfulness of processing are correct, except:

A. Processing is necessary for the performance of a contract to which the data subject is party

B. Processing is necessary to obtain consent from the data subject

C. Processing is necessary to protect the vital interests of the data subject or of another natural person

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

A shop owner decided to install a video surveillance system to protect the property against theft. However, the cameras also capture a considerable part of the store next by. Which statement below is correct in this case?

A. Controllers or processors that provide the means of processing personal data for such activities should operate under the requirements community privacy

B. This provision does not fall under the GDPR requirements as it does not pose a high threat to the rights and freedoms of data subjects

C. Controllers or processors of personal data under this provision fall under the GDPR, since the cameras should capture only the premises of the shop owner who installed the cameras in the first place

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

According to the principle of data minimization, data must be:

A. In a form which permits the identification of data subjects for no longer than is necessary

B. Acquired only for specified, explicit, and legitimate purposes

C. Adequate, relevant, and limited to what is necessary in relation to the purposes of processing

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Bankbio is a financial institution that handles personal data of its customers. Its data processing activities involve processing that is necessary for the purposes of the legitimate interests pursued by the institution. In such cases, Bankbio processes personal data without obtaining consent by data subjects. Is the data processing considered lawful in this case?

A. Yes, processing is lawful when it is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests of fundamental rights

B. No, the processing is lawful only if the data subject has given explicit consent to the processing of personal data for the specified purpose

C. Yes, GDPR allows the processing of personal data for the purposes of the legitimate interest pursued by the controller or by a third party in all cases

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

According to Article 82 of the GDPR, when must the processor be held liable for the damage caused by processing?

A. Only when it has not complied with the data subject's requirements

B. Only when it has acted outside of or contrary to the lawful instructions of the controller

C. Only when the processing of data has not been done based on the instructions received by the organization's DPO

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Pinky is a leading accessories brand that produces necklaces, rings, earrings, and bracelets. After opening a new shop in Italy, Pinky wanted to analyze their business performance. This required the collection of purchases of customers from all the shops, whereas the identification of customers was not necessary. Should Pinky process additional information from customers in order to identify data subjects as requested by the GDPR?

A. Yes, Pinky is required to maintain, acquire, or process additional information in order to identify the data subject

B. Yes, Pinky required to process additional information for the purpose of exercising the data subject rights covered in Articles 15-21 of GDPR

C. No, Pinky is not required to process additional information, since the processing of personal data in this case does not require Pinky to identify the data subject

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!