

CIPP-E Dumps

Certified Information Privacy Professional/Europe (CIPP/E)

<https://www.certleader.com/CIPP-E-dumps.html>



NEW QUESTION 1

SCENARIO

Please use the following to answer the next question:

ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.

Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain's locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.

Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.

What are ABC Hotel Chain and XYZ Travel Agency's roles in this relationship?

- A. ABC Hotel Chain is the controller and XYZ Travel Agency is the processor.
- B. XYZ Travel Agency is the controller and ABC Hotel Chain is the processor.
- C. ABC Hotel Chain and XYZ Travel Agency are independent controllers.
- D. ABC Hotel Chain and XYZ Travel Agency are joint controllers.

Answer: A

NEW QUESTION 2

With the issue of consent, the GDPR allows member states some choice regarding what?

- A. The mechanisms through which consent may be communicated
- B. The circumstances in which silence or inactivity may constitute consent
- C. The age at which children must be required to obtain parental consent
- D. The timeframe in which data subjects are allowed to withdraw their consent

Answer: C

NEW QUESTION 3

To which of the following parties does the territorial scope of the GDPR NOT apply?

- A. All member countries of the European Economic Area.
- B. All member countries party to the Treaty of Lisbon.
- C. All member countries party to the Paris Agreement.
- D. All member countries of the European Union.

Answer: A

NEW QUESTION 4

Which sentence best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

- A. Employees must sign an ad hoc contractual agreement each time personal data is exported.
- B. All employees are subject to the rules in their entirety, regardless of where the work is taking place.
- C. All employees must follow the privacy regulations of the jurisdictions where the current scope of their work is established.
- D. Employees who control personal data must complete a rigorous certification procedure, as they are exempt from legal enforcement.

Answer: C

NEW QUESTION 5

According to the European Data Protection Board, which of the following concepts or practices does NOT follow from the principles relating to the processing of personal data under EU data protection law?

- A. Data ownership allocation.
- B. Access control management.
- C. Frequent pseudonymization key rotation.
- D. Error propagation avoidance along the processing chain.

Answer: C

NEW QUESTION 6

According to Article 84 of the GDPR, the rules on penalties applicable to infringements shall be laid down by?

- A. The local Data Protection Supervisory Authorities.
- B. The European Data Protection Board.
- C. The EU Commission.
- D. The Member States.

Answer: D

NEW QUESTION 7

SCENARIO

Please use the following to answer the next QUESTION NO:

Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by

texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.

Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.

In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.

Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system. Based on the GDPR's position on the use of personal data for direct marketing purposes, which of the following is true about Louis's rights as a data subject?

- A. Louis does not have the right to object to the use of his data because he previously consented to it.
- B. Louis has the right to object at any time to the use of his data and Bedrock must honor his request to cease use.
- C. Louis has the right to object to the use of his data, unless his data is required by Bedrock for the purpose of exercising a legal claim.
- D. Louis does not have the right to object to the use of his data if Bedrock can demonstrate compelling legitimate grounds for the processing.

Answer: B

NEW QUESTION 8

Please use the following to answer the next question:

WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data

provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information.

The privacy statement on Wonderkids' website states the following:

"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the data. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information. We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."

"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."

"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities."

What direct marketing information can WonderKids send by email without prior consent of the person booking the childcare?

- A. No marketing information at all.
- B. Any marketing information at all.
- C. Marketing information related to other business operations of WonderKids.
- D. Marketing information for products or services similar to those purchased from WonderKids.

Answer: C

NEW QUESTION 9

Which of the following does NOT have to be included in the records most processors must maintain in relation to their data processing activities?

- A. Name and contact details of each controller on behalf of which the processor is acting.
- B. Categories of processing carried out on behalf of each controller for which the processor is acting.
- C. Details of transfers of personal data to a third country carried out on behalf of each controller for which the processor is acting.
- D. Details of any data protection impact assessment conducted in relation to any processing activities carried out by the processor on behalf of each controller for which the processor is acting.

Answer: C

NEW QUESTION 10

Which area of privacy is a lead supervisory authority's (LSA) MAIN concern?

- A. Data subject rights
- B. Data access disputes
- C. Cross-border processing
- D. Special categories of data

Answer: C

NEW QUESTION 10

To receive a preliminary interpretation on provisions of the GDPR, a national court will refer its case to which of the following?

- A. The Court of Justice of the European Union.
- B. The European Data Protection Supervisor.
- C. The European Court of Human Rights.
- D. The European Data Protection Board.

Answer: A

NEW QUESTION 11

SCENARIO

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

Registration Form

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)

Vigotron values your privacy. The M-Health app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)

Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third-party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

We are happy to offer the M-Health app free of charge. If you want to download and use it, we ask that you first complete this registration form. (Please note that use of the M-Health app is restricted to adults aged 16 or older, unless parental consent has been given to minors intending to use it.)

First name:

Surname:

Year of birth:

Email:

Physical Address (optional*):

Health status:

*If you are interested in receiving newsletters about our products and services that we think may be of interest to you, please include your physical address. If you decide later that you do not wish to receive these newsletters, you can unsubscribe by sending an email to unsubscribe@vigotron.com or send a letter with your request to the address listed at the bottom of this page.

Terms and Conditions 1.Jurisdiction. [...] 2.Applicable law. [...] 3.Limitation of liability. [...] Consent

By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.

If a user of the M-Health app were to decide to withdraw his consent, Vigotron would first be required to do what?

- A. Provide the user with logs of data collected through use of the app.
- B. Erase any data collected from the time the app was first used.
- C. Inform any third parties of the user's withdrawal of consent.
- D. Cease processing any data collected through use of the app.

Answer: D

NEW QUESTION 14

SCENARIO

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased. Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization. To comply with the GDPR, what should Building Block have done as a first step before implementing the SecurityScan measure?

- A. Assessed potential privacy risks by conducting a data protection impact assessment.
- B. Consulted with the relevant data protection authority about potential privacy violations.
- C. Distributed a more comprehensive notice to employees and received their express consent.
- D. Consulted with the Information Security team to weigh security measures against possible server impacts.

Answer: C

NEW QUESTION 16

What type of data lies beyond the scope of the General Data Protection Regulation?

- A. Pseudonymized
- B. Anonymized
- C. Encrypted
- D. Masked

Answer: B

NEW QUESTION 21

When hiring a data processor, which action would a data controller NOT be able to depend upon to avoid liability in the event of a security breach?

- A. Documenting due diligence steps taken in the pre-contractual stage.
- B. Conducting a risk assessment to analyze possible outsourcing threats.
- C. Requiring that the processor directly notify the appropriate supervisory authority.
- D. Maintaining evidence that the processor was the best possible market choice available.

Answer: A

NEW QUESTION 25

Article 9 of the GDPR lists exceptions to the general prohibition against processing biometric data. Which of the following is NOT one of these exceptions?

- A. The processing is done by a non-profit organization and the results are disclosed outside the organization.
- B. The processing is necessary to protect the vital interests of the data subject when he or she is incapable of giving consent.
- C. The processing is necessary for the establishment, exercise or defense of legal claims when courts are acting in a judicial capacity.
- D. The processing is explicitly consented to by the data subject and he or she is allowed by Union or Member State law to lift the prohibition.

Answer: A

NEW QUESTION 28

In which of the following situations would an individual most likely to be able to withdraw her consent for processing?

- A. When she is leaving her bank and moving to another bank.
- B. When she has recently changed jobs and no longer works for the same company.
- C. When she disagrees with a diagnosis her doctor has recorded on her records.
- D. When she no longer wishes to be sent marketing materials from an organization.

Answer: D

NEW QUESTION 32

How does the GDPR now define "processing"?

- A. Any act involving the collecting and recording of personal data.
- B. Any operation or set of operations performed on personal data or on sets of personal data.
- C. Any use or disclosure of personal data compatible with the purpose for which the data was collected.
- D. Any operation or set of operations performed by automated means on personal data or on sets of personal data.

Answer: A

NEW QUESTION 33

Which of the following is NOT considered a fair processing practice in relation to the transparency principle?

- A. Providing a multi-layered privacy notice, in a website environment.
- B. Providing a QR code linking to more detailed privacy notice, in a CCTV sign.
- C. Providing a hyperlink to the organization's home page, in a hard copy application form.
- D. Providing a "just-in-time" contextual pop-up privacy notice, in an online application from field.

Answer: A

NEW QUESTION 36

SCENARIO

Please use the following to answer the next question:

Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.

Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.

The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre-registrations, it will develop EU-specific content and services.

Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.

The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.

On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.

If Who-R-U decides to track locations using its app, what must it do to comply with the GDPR?

- A. Get consent from the app users.
- B. Provide a transparent notice to users.
- C. Anonymize the data and add latency so it avoids disclosing real time locations.
- D. Obtain a court order because location data is a special category of personal data.

Answer: A

NEW QUESTION 41

A multinational company is appointing a mandatory data protection officer. In addition to considering the rules set out in Article 37 (1) of the GDPR, which of the following actions must the company also undertake to ensure compliance in all EU jurisdictions in which it operates?

- A. Consult national derogations to evaluate if there are additional cases to be considered in relation to the matter.
- B. Conduct a Data Protection Privacy Assessment on the processing operations of the company in all the countries it operates.
- C. Assess whether the company has more than 250 employees in each of the EU member-states in which it is established.
- D. Revise the data processing activities of the company that affect more than one jurisdiction to evaluate whether they comply with the principles of privacy by design and by default.

Answer: B

NEW QUESTION 43

A U.S.-based online shop uses sophisticated software to track the browsing behavior of its European customers and predict future purchases. It also shares this information with third parties. Under the GDPR, what is the online shop's PRIMARY obligation while engaging in this kind of profiling?

- A. It must solicit informed consent through a notice on its website
- B. It must seek authorization from the European supervisory authorities
- C. It must be able to demonstrate a prior business relationship with the customers
- D. It must prove that it uses sufficient security safeguards to protect customer data

Answer: A

NEW QUESTION 48

Which of the following was the first legally binding international instrument in the area of data protection?

- A. Convention 108.
- B. General Data Protection Regulation.
- C. Universal Declaration of Human Rights.
- D. EU Directive on Privacy and Electronic Communications.

Answer: A

NEW QUESTION 51

What is the MAIN reason GDPR Article 4(22) establishes the concept of the "concerned supervisory authority"?

- A. To encourage the consistency of local data processing activity.
- B. To give corporations a choice about who their supervisory authority will be.
- C. To ensure the GDPR covers controllers that do not have an establishment in the EU but have a representative in a member state.
- D. To ensure that the interests of individuals residing outside the lead authority's jurisdiction are represented.

Answer: A

NEW QUESTION 54

If a multi-national company wanted to conduct background checks on all current and potential employees, including those based in Europe, what key provision would the company have to follow?

- A. Background checks on employees could be performed only under prior notice to all employees.
- B. Background checks are only authorized with prior notice and express consent from all employees including those based in Europe.
- C. Background checks on European employees will stem from data protection and employment law, which can vary between member states.
- D. Background checks may not be allowed on European employees, but the company can create lists based on its legitimate interests, identifying individuals who are ineligible for employment.

Answer: C

NEW QUESTION 56

Assuming that the “without undue delay” provision is followed, what is the time limit for complying with a data access request?

- A. Within 40 days of receipt
- B. Within 40 days of receipt, which may be extended by up to 40 additional days
- C. Within one month of receipt, which may be extended by up to an additional month
- D. Within one month of receipt, which may be extended by an additional two months

Answer: C

NEW QUESTION 59

SCENARIO

Please use the following to answer the next question:

Zandelay Fashion (‘Zandelay’) is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company’s compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.

The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.

In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company’s customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures. Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay’s business plan and associated processing activities.

What must Zandelay provide to the supervisory authority during the prior consultation?

- A. An evaluation of the complexity of the intended processing.
- B. An explanation of the purposes and means of the intended processing.
- C. Records showing that customers have explicitly consented to the intended profiling activities.
- D. Certificates that prove Martin’s professional qualities and expert knowledge of data protection law.

Answer: B

NEW QUESTION 61

SCENARIO

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick’s instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients’ data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft’s engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies’ websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem’s as well as EcoMick’s latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem’s products, she has never shopped EcoMick, nor provided her personal data to that company.

Why would the consent provided by Ms. Iman NOT be considered valid in regard to JaphSoft?

- A. She was not told which controller would be processing her personal data.
- B. She only viewed the visual representations of the privacy notice Liem provided.
- C. She did not read the privacy notice stating that her personal data would be shared.
- D. She has never made any purchases from JaphSoft and has no relationship with the company.

Answer: C

NEW QUESTION 66

Under Article 58 of the GDPR, which of the following describes a power of supervisory authorities in European Union (EU) member states?

- A. The ability to enact new laws by executive order.
- B. The right to access data for investigative purposes.
- C. The discretion to carry out goals of elected officials within the member state.
- D. The authority to select penalties when a controller is found guilty in a court of law.

Answer: B

NEW QUESTION 68

An entity's website stores text files on EU users' computer and mobile device browsers. Prior to doing so, the entity is required to provide users with notices containing information and consent under which of the following frameworks?

- A. General Data Protection Regulation 2016/679.
- B. E-Privacy Directive 2002/58/EC.
- C. E-Commerce Directive 2000/31/EC.
- D. Data Protection Directive 95/46/EC.

Answer: D

NEW QUESTION 72**SCENARIO**

Please use the following to answer the next question:

Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA. Today, it is a multi-billion-dollar candy company operating in every continent. All of the company's IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father's company, but is also secretly working on launching a new global online dating website company called Ben Knows Best.

Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company's online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers' philosophical beliefs, political opinions and marital status.

If a customer identifies as single, Ben then copies all of that customer's personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out.

Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Break with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.

Joe also hires his best friend's daughter, Alice, who just graduated from law school in the U.S., to be the company's new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company's operations in the European Union to the U.S.

Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company's IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone's information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.

As a result of Sam's actions, the Gummy Bear Company potentially violated Articles 33 and 34 of the GDPR and will be required to do what?

- A. Notify its Data Protection Authority about the data breach.
- B. Analyze and evaluate the liability for customers in Ireland.
- C. Analyze and evaluate all of its breach notification obligations.
- D. Notify all of its customers that reside in the European Union.

Answer: A

NEW QUESTION 74**SCENARIO**

Please use the following to answer the next question:

Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.

Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.

The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre-registrations, it will develop EU-specific content and services.

Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.

The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.

On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.

Who-R-U is NOT required to notify the local German DPA about the laptop theft because?

- A. The company isn't a controller established in the Union.
- B. The laptop belonged to a company located in Canada.
- C. The data isn't considered personally identifiable financial information.
- D. There is no evidence that the thieves have accessed the data on the laptop.

Answer: A

NEW QUESTION 78

SCENARIO

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased. Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.

What would be the MOST APPROPRIATE way for Building Block to handle the situation with the employee from Italy?

- A. Since the GDPR does not apply to this situation, the company would be entitled to apply any disciplinary measure authorized under Italian labor law.
- B. Since the employee was the cause of a serious risk for the server performance and their data, the company would be entitled to apply disciplinary measures to this employee, including fair dismissal.
- C. Since the employee was not informed that the security measures would be used for other purposes such as monitoring, the company could face difficulties in applying any disciplinary measures to this employee.
- D. Since this was a serious infringement, but the employee was not appropriately informed about the consequences the new security measures, the company would be entitled to apply some disciplinary measures, but not dismissal.

Answer: D

NEW QUESTION 80

How is the GDPR's position on consent MOST likely to affect future app design and implementation?

- A. App developers will expand the amount of data necessary to collect for an app's functionality.
- B. Users will be given granular types of consent for particular types of processing.
- C. App developers' responsibilities as data controllers will increase.
- D. Users will see fewer advertisements when using apps.

Answer: B

NEW QUESTION 84

Bioface is a company based in the United States. It has no servers, personnel or assets in the European Union. By collecting photographs from social media and other web-based services, such as newspapers and blogs, it uses machine learning to develop a facial recognition algorithm. The algorithm identifies individuals in photographs who are not in its data set based the algorithm and its existing data. The service collects photographs of data subjects in the European Union and will identify them if presented with their photographs. Bioface offers its service to government agencies and companies in the United States and Canada, but not to those in the European Union. Bioface does not offer the service to individuals.

Why is Bioface subject to the territorial scope of the General Data Protection Regulation?

- A. It collects data from European Union websites, which constitutes an establishment in the European Union.
- B. It offers services in the European Union by identifying data subjects in the European Union.
- C. It collects data from subjects and uses it for automated processing.
- D. It monitors the behavior of data subjects in the European Union.

Answer: A

NEW QUESTION 86**SCENARIO**

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.

Which of the following BEST describes the relationship between Liem, EcoMick and JaphSoft?

- A. Liem is a controller and EcoMick is a processor because Liem provides specific instructions regarding how the marketing campaigns should be rolled out.
- B. EcoMick and JaphSoft are is a controller and Liem is a processor because EcoMick is sharing its marketing data with Liem for contacts in Europe.
- C. JaphSoft is the sole processor because it processes personal data on behalf of its clients.
- D. Liem and EcoMick are joint controllers because they carry out joint marketing activities.

Answer: B

NEW QUESTION 87

Which of the following would MOST likely trigger the extraterritorial effect of the GDPR, as specified by Article 3?

- A. The behavior of suspected terrorists being monitored by EU law enforcement bodies.
- B. Personal data of EU citizens being processed by a controller or processor based outside the EU.
- C. The behavior of EU citizens outside the EU being monitored by non-EU law enforcement bodies.
- D. Personal data of EU residents being processed by a non-EU business that targets EU customers.

Answer: B

NEW QUESTION 88**SCENARIO**

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third-party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated.

Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.

Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box's home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box's Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.

Despite some customer complaints, Brady's business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad network with whom he has set clearly defined roles. Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and services.

Under the General Data Protection Regulation (GDPR), what is the most likely reason Serge may have grounds to object to the use of his quotation?

- A. Because of the misrepresentation of personal data as an endorsement.
- B. Because of the juxtaposition of the quotation with others' quotations.
- C. Because of the use of personal data outside of the social networking service (SNS).
- D. Because of the misapplication of the household exception in relation to a social networking service (SNS).

Answer: D

NEW QUESTION 93**SCENARIO**

Please use the following to answer the next question:

WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids' website states the following:

"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the data. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information.

We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."

"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."

"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities."

What must the contract between WonderKids and the hosting service provider contain?

- A. The requirement to implement technical and organizational measures to protect the data.
- B. Controller-to-controller model contract clauses.
- C. Audit rights for the data subjects.
- D. A non-disclosure agreement.

Answer: A

NEW QUESTION 94

When collecting personal data in a European Union (EU) member state, what must a company do if it collects personal data from a source other than the data subjects themselves?

- A. Inform the subjects about the collection
- B. Provide a public notice regarding the data

- C. Upgrade security to match that of the source
- D. Update the data within a reasonable timeframe

Answer: A

NEW QUESTION 98

A company in France suffers a robbery over the weekend owing to a faulty alarm system. When it is determined that the break-in involves the loss of a substantial amount of data, the company decides on a CCTV system to monitor for future incidents. Company technicians install cameras in the entrance of the building, hallways and offices. Footage is recorded continuously, and is monitored by the home office in the United States. What is the most realistic step the company could take to address their security concerns and comply with the personal data processing principles set out in Article 5 of the GDPR?

- A. Seek informed consent from company employees.
- B. Have cameras recording during work hours only.
- C. Retain captured footage for no more than 30 days.
- D. Restrict camera placement to building entrances only.

Answer: A

NEW QUESTION 100

When may browser settings be relied upon for the lawful application of cookies?

- A. When a user rejects cookies that are strictly necessary.
- B. When users are aware of the ability to adjust their settings.
- C. When users are provided with information about which cookies have been set.
- D. When it is impossible to bypass the choices made by users in their browser settings.

Answer: B

NEW QUESTION 102

If a data subject puts a complaint before a DPA and receives no information about its progress or outcome, how long does the data subject have to wait before taking action in the courts?

- A. 1 month.
- B. 3 months.
- C. 5 months.
- D. 12 months.

Answer: B

NEW QUESTION 104

In 2016's Guidance, the United Kingdom's Information Commissioner's Office (ICO) reaffirmed the importance of using a "layered notice" to provide data subjects with what?

- A. A privacy notice containing brief information whilst offering access to further detail.
- B. A privacy notice explaining the consequences for opting out of the use of cookies on a website.
- C. An explanation of the security measures used when personal data is transferred to a third party.
- D. An efficient means of providing written consent in member states where they are required to do so.

Answer: A

NEW QUESTION 107

An organisation receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal data. Under what condition can the organisation charge the data subject for processing the request?

- A. Only where the organisation can show that it is reasonable to do so because more than one request was made.
- B. Only to the extent this is allowed under the restrictions on data subjects' rights introduced under Art 23 of GDPR.
- C. Only where the administrative costs of taking the action requested exceeds a certain threshold.
- D. Only if the organisation can demonstrate that the request is clearly excessive or misguided.

Answer: D

NEW QUESTION 108

A mobile device application that uses cookies will be subject to the consent requirement of which of the following?

- A. The ePrivacy Directive
- B. The E-Commerce Directive
- C. The Data Retention Directive
- D. The EU Cybersecurity Directive

Answer: A

NEW QUESTION 110

Which GDPR principle would a Spanish employer most likely depend upon to annually send the personal data of its employees to the national tax authority?

- A. The consent of the employees.

- B. The legal obligation of the employer.
- C. The legitimate interest of the public administration.
- D. The protection of the vital interest of the employees.

Answer: B

NEW QUESTION 113

SCENARIO

Please use the following to answer the next question:

T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.

T-Craze also opened various office locations throughout Europe to help expand its business. While Germany Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T-Craze, though with much less success.

The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.

What is the best option for the lead regulator when responding to the Spanish supervisory authority's notice that it plans to take action regarding Sofia's complaint?

- A. Accept, because it did not receive any complaints.
- B. Accept, because GDPR permits non-lead authorities to take action for such complaints.
- C. Reject, because Right Target's processing was conducted throughout Europe.
- D. Reject, because GDPR does not allow other supervisory authorities to take action if there is a lead authority.

Answer: D

NEW QUESTION 117

Under Article 21 of the GDPR, a controller must stop profiling when requested by a data subject, unless it can demonstrate compelling legitimate grounds that override the interests of the individual. In the Guidelines on Automated individual decision-making and Profiling, the WP 29 says the controller needs to do all of the following to demonstrate that it has such legitimate grounds EXCEPT?

- A. Carry out an exercise that weighs the interests of the controller and the basis for the data subject's objection.
- B. Consider the impact of the profiling on the data subject's interest, rights and freedoms.
- C. Demonstrate that the profiling is for the purposes of direct marketing.
- D. Consider the importance of the profiling to their particular objective.

Answer: C

NEW QUESTION 120

An organization receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal data. Under what condition can the organization charge the data subject a fee for processing the request?

- A. Only where the organization can show that it is reasonable to do so because more than one request was made.
- B. Only to the extent this is allowed under the restrictions on data subjects' rights introduced under Art 23 of GDPR.
- C. Only where the administrative costs of taking the action requested exceeds a certain threshold.
- D. Only if the organization can demonstrate that the request is clearly excessive or misguided.

Answer: B

NEW QUESTION 125

SCENARIO

Please use the following to answer the next question:

Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.

The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.

In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures, Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.

What would MOST effectively assist Zandelay in conducting their data protection impact assessment?

- A. Information about DPIAs found in Articles 38 through 40 of the GDPR.
- B. Data breach documentation that data controllers are required to maintain.
- C. Existing DPIA guides published by local supervisory authorities.
- D. Records of processing activities that data controllers are required to maintain.

Answer: A

NEW QUESTION 130

SCENARIO

Please use the following to answer the next question:

T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.

T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze's headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T-Craze, though with much less success.

The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.

Why does the Spanish supervisory authority notify the French supervisory authority when it opens an investigation into T-Craze based on Sofia's complaint?

- A. T-Craze has a French affiliate.
- B. The French affiliate procured the services of Right Target.
- C. T-Craze conducts its marketing and sales activities in France.
- D. The Spanish supervisory authority is providing a courtesy notification not required under the GDPR.

Answer: C

NEW QUESTION 132

Which GDPR requirement will present the most significant challenges for organizations with Bring Your Own Device (BYOD) programs?

- A. Data subjects must be sufficiently informed of the purposes for which their personal data is processed.
- B. Processing of special categories of personal data on a large scale requires appointing a DPO.
- C. Personal data of data subjects must always be accurate and kept up to date.
- D. Data controllers must be in control of the data they hold at all times.

Answer: D

NEW QUESTION 134

Which of the following is NOT recognized as being a common characteristic of cloud-computing services?

- A. The service's infrastructure is shared among the supplier's customers and can be located in a number of countries.
- B. The supplier determines the location, security measures, and service standards applicable to the processing.
- C. The supplier allows customer data to be transferred around the infrastructure according to capacity.
- D. The supplier assumes the vendor's business risk associated with data processed by the supplier.

Answer: D

NEW QUESTION 136**SCENARIO**

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

Registration Form

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)

Vigotron values your privacy. The M-Health app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)

Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third-party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

We are happy to offer the M-Health app free of charge. If you want to download and use it, we ask that you first complete this registration form. (Please note that use of the M-Health app is restricted to adults aged 16 or older, unless parental consent has been given to minors intending to use it.)

First name:

Surname:

Year of birth:

Email:

Physical Address (optional*):

Health status:

*If you are interested in receiving newsletters about our products and services that we think may be of interest to you, please include your physical address. If you decide later that you do not wish to receive these newsletters, you can unsubscribe by sending an email to unsubscribe@vigotron.com or send a letter with your request to the address listed at the bottom of this page.

Terms and Conditions 1. Jurisdiction. [...] 2. Applicable law. [...] 3. Limitation of liability. [...] Consent

By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.

What is one potential problem Vigotron's age policy might encounter under the GDPR?

- A. Age restrictions are more stringent when health data is involved.

- B. Users are only required to be aged 13 or over to be considered adults.
- C. Organizations must make reasonable efforts to verify parental consent.
- D. Organizations that tie a service to marketing must seek consent for each purpose.

Answer: A

NEW QUESTION 140

What term BEST describes the European model for data protection?

- A. Sectoral
- B. Self-regulatory
- C. Market-based
- D. Comprehensive

Answer: A

NEW QUESTION 143

SCENARIO

Please use the following to answer the next question:

Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.

Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.

In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.

Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system. Which statement accurately summarizes Bedrock's obligation in regard to Louis's data portability request?

- A. Bedrock does not have a duty to transfer Louis's data to Zantrum if doing so is legitimately not technically feasible.
- B. Bedrock does not have to transfer Louis's data to Zantrum because the right to data portability does not apply where personal data are processed in order to carry out tasks in the public interest.
- C. Bedrock has failed to comply with the duty to transfer Louis's data to Zantrum because the duty applies wherever personal data are processed by automated means and necessary for the performance of a contract with the customer.
- D. Bedrock has failed to comply with the duty to transfer Louis's data to Zantrum because it has an obligation to develop commonly used, machine-readable and interoperable formats so that all customer data can be ported to other insurers on request.

Answer: B

NEW QUESTION 147

As a result of the European Court of Justice's ruling in the case of Google v. Spain, search engines outside the EEA are also likely to be subject to the Regulation's right to be forgotten. This holds true if the activities of an EU subsidiary and its U.S. parent are what?

- A. Supervised by the same Data Protection Officer.
- B. Consistent with Privacy Shield requirements
- C. Bound by a standard contractual clause.
- D. Inextricably linked in their businesses.

Answer: D

NEW QUESTION 150

What was the aim of the European Data Protection Directive 95/46/EC?

- A. To harmonize the implementation of the European Convention of Human Rights across all member states.
- B. To implement the OECD Guidelines on the Protection of Privacy and trans-border flows of Personal Data.
- C. To completely prevent the transfer of personal data out of the European Union.
- D. To further reconcile the protection of the fundamental rights of individuals with the free flow of data from one member state to another.

Answer: B

NEW QUESTION 154

What permissions are required for a marketer to send an email marketing message to a consumer in the EU?

- A. A prior opt-in consent for consumers unless they are already customers.
- B. A pre-checked box stating that the consumer agrees to receive email marketing.

- C. A notice that the consumer's email address will be used for marketing purposes.
- D. No prior permission required, but an opt-out requirement on all emails sent to consumers.

Answer: A

NEW QUESTION 158

WP29's "Guidelines on Personal data breach notification under Regulation 2016/679" provides examples of ways to communicate data breaches transparently. Which of the following was listed as a method that would NOT be effective for communicating a breach to data subjects?

- A. A postal notification
- B. A direct electronic message
- C. A notice on a corporate blog
- D. A prominent advertisement in print media

Answer: C

NEW QUESTION 163

Under what circumstances would the GDPR apply to personal data that exists in physical form, such as information contained in notebooks or hard copy files?

- A. Only where the personal data is produced as a physical output of specific automated processing activities, such as printing, labelling, or stamping.
- B. Only where the personal data is to be subjected to specific computerized processing, such as image scanning or optical character recognition.
- C. Only where the personal data is treated by automated means in some way, such as computerized distribution or filing.
- D. Only where the personal data is handled in a sufficiently structured manner so as to form part of a filing system.

Answer: D

NEW QUESTION 167

A key component of the OECD Guidelines is the "Individual Participation Principle". What parts of the General Data Protection Regulation (GDPR) provide the closest equivalent to that principle?

- A. The lawful processing criteria stipulated by Articles 6 to 9
- B. The information requirements set out in Articles 13 and 14
- C. The breach notification requirements specified in Articles 33 and 34
- D. The rights granted to data subjects under Articles 12 to 22

Answer: D

NEW QUESTION 169

A data controller appoints a data protection officer. Which of the following conditions would NOT result in an infringement of Articles 37 to 39 of the GDPR?

- A. If the data protection officer lacks ISO 27001 auditor certification.
- B. If the data protection officer is provided by the data processor.
- C. If the data protection officer also manages the marketing budget.
- D. If the data protection officer receives instructions from the data controller.

Answer: D

NEW QUESTION 171

SCENARIO

Please use the following to answer the next question:

BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information – name, location, and prior purchase history – with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens.

Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.

In which case would Natural Insight's use of BHealthy's data for improvement of its algorithms be considered data processor activity?

- A. If Natural Insight uses BHealthy's data for improving price point predictions only for BHealthy.
- B. If Natural Insight receives express contractual instructions from BHealthy to use its data for improving its algorithms.
- C. If Natural Insight agrees to be fully liable for its use of BHealthy's customer information in its product improvement activities.
- D. If Natural Insight satisfies the transparency requirement by notifying BHealthy's customers of its plans to use their information for its product improvement activities.

Answer: A

NEW QUESTION 173

SCENARIO

Please use the following to answer the next question:

Sandy recently joined Market4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.

Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.

What should Sandy give as feedback to Dan and the marketing team regarding the new fields Dan wants to add to Market4U's forms?

- A. Make all the fields optional.
- B. Only request the information in brackets (i.e., age group and salary range).
- C. Eliminate the fields, as they are not proportional to the services being offered.
- D. Eliminate the fields as they are not necessary for the purposes of providing white papers or registration for events.

Answer: D

NEW QUESTION 177

Which of the following is one of the supervisory authority's investigative powers?

- A. To notify the controller or the processor of an alleged infringement of the GDPR.
- B. To require that controllers or processors adopt approved data protection certification mechanisms.
- C. To determine whether a controller or processor has the right to a judicial remedy concerning a compensation decision made against them.
- D. To require data controllers to provide them with written notification of all new processing activities.

Answer: A

NEW QUESTION 182

The GDPR specifies fines that may be levied against data controllers for certain infringements. Which of the following infringements would be subject to the less severe administrative fine of up to 10 million euros (or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year)?

- A. Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing.
- B. Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default.
- C. Failure to process personal information in a manner compatible with its original purpose.
- D. Failure to provide the means for a data subject to rectify inaccuracies in personal data.

Answer: D

NEW QUESTION 185

Which of the following was the first to implement national law for data protection in 1973?

- A. France
- B. Sweden
- C. Germany
- D. United Kingdom

Answer: B

NEW QUESTION 190

When is data sharing agreement MOST likely to be needed?

- A. When anonymized data is being shared.
- B. When personal data is being shared between commercial organizations acting as joint data controllers.
- C. When personal data is being proactively shared by a controller to support a police investigation.
- D. When personal data is being shared with a public authority with powers to require the personal data to be disclosed.

Answer: B

NEW QUESTION 194

SCENARIO

Please use the following to answer the next question:

Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.

Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.

The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre-registrations, it will develop EU-specific content and services.

Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.

The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.

On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.

The Customer for Life plan may conflict with which GDPR provision?

- A. Article 6, which requires processing to be lawful.
- B. Article 7, which requires consent to be as easy to withdraw as it is to give.
- C. Article 16, which provides data subjects with a rights to rectification.
- D. Article 20, which gives data subjects a right to data portability.

Answer: B

NEW QUESTION 198

Which of the following would NOT be relevant when determining if a processing activity would be considered profiling?

- A. If the processing is to be performed by a third-party vendor
- B. If the processing involves data that is considered personal data
- C. If the processing of the data is done through automated means
- D. If the processing is used to predict the behavior of data subjects

Answer: D

NEW QUESTION 199

SCENARIO

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

Registration Form

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)

Vigotron values your privacy. The M-Health app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)

Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third-party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

We are happy to offer the M-Health app free of charge. If you want to download and use it, we ask that you first complete this registration form. (Please note that use of the M-Health app is restricted to adults aged 16 or older, unless parental consent has been given to minors intending to use it.)

First name:

Surname:

Year of birth:

Email:

Physical Address (optional*):

Health status:

*If you are interested in receiving newsletters about our products and services that we think may be of interest to you, please include your physical address. If you decide later that you do not wish to receive these newsletters, you can unsubscribe by sending an email to unsubscribe@vigotron.com or send a letter with your request to the address listed at the bottom of this page.

Terms and Conditions 1.Jurisdiction. [...] 2.Applicable law. [...] 3.Limitation of liability. [...] Consent

By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.

Emily sends the draft to Sam for review. Which of the following is Sam most likely to point out as the biggest problem with Emily's consent provision?

- A. It is not legal to include fields requiring information regarding health status without consent.
- B. Processing health data requires explicit consent, but the form does not ask for explicit consent.
- C. Direct marketing requires explicit consent, whereas the registration form only provides for a right to object
- D. The provision of the fitness app should be made conditional on the consent to the data processing for direct marketing.

Answer: C

NEW QUESTION 204

What is the key difference between the European Council and the Council of the European Union?

- A. The Council of the European Union is helmed by a president.
- B. The Council of the European Union has a degree of legislative power.
- C. The European Council focuses primarily on issues involving human rights.
- D. The European Council is comprised of the heads of each EU member state.

Answer: D

NEW QUESTION 208

Based on GDPR Article 35, which of the following situations would trigger the need to complete a DPIA?

- A. A company wants to combine location data with other data in order to offer more personalized service for the customer.
- B. A company wants to use location data to infer information on a person's clothes purchasing habits.
- C. A company wants to build a dating app that creates candidate profiles based on location data and data from third-party sources.
- D. A company wants to use location data to track delivery trucks in order to make the routes more efficient.

Answer: C

NEW QUESTION 211

What is an important difference between the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) in relation to their roles and functions?

- A. ECHR can rule on issues concerning privacy as a fundamental right, while the CJEU cannot.
- B. CJEU can force national governments to implement and honor EU law, while the ECHR cannot.
- C. CJEU can hear appeals on human rights decisions made by national courts, while the ECHR cannot.
- D. ECHR can enforce human rights laws against governments that fail to implement them, while the CJEU cannot.

Answer: B

NEW QUESTION 216

Many businesses print their employees' photographs on building passes, so that employees can be identified by security staff. This is notwithstanding the fact that facial images potentially qualify as biometric data under the GDPR. Why would such practice be permitted?

- A. Because use of biometric data to confirm the unique identification of data subjects benefits from an exemption.
- B. Because photographs qualify as biometric data only when they undergo a "specific technical processing".
- C. Because employees are deemed to have given their explicit consent when they agree to be photographed by their employer.
- D. Because photographic ID is a physical security measure which is "necessary for reasons of substantial public interest".

Answer: B

Explanation:

Reference https://ess.csa.canon.com/rs/206-CLL-191/images/IAPP-Top-10-Operational-Impacts-of-GDPR.pdf?TC=DM&CN=CSA_OMNIA_Partners&CS=CSA&CR=T1_Gov%20GenNonProfit (11)

NEW QUESTION 219

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CIPP-E Exam with Our Prep Materials Via below:

<https://www.certleader.com/CIPP-E-dumps.html>