IAPP

Exam Questions CIPP-E

Certified Information Privacy Professional/Europe (CIPP/E)

NEW QUESTION 1
In the event of a data breach, which type of information are data controllers NOT required to provide to either the supervisory authorities or the data subjects?

A. The predicted consequences of the breach.
B. The measures being taken to address the breach.
C. The type of security safeguards used to protect the data.
D. The contact details of the appropriate data protection officer.

Answer: D

NEW QUESTION 2
If a French controller has a car-sharing app available only in Morocco, Algeria and Tunisia, but the data processing activities are carried out by the appointed processor in Spain, the GDPR will apply to the processing of the personal data so long as?

A. The individuals are European citizens or residents.
B. The data processing activities are in Spain.
C. The data controller is in France.
D. The EU individuals are targeted.

Answer: D

NEW QUESTION 3
What must be included in a written agreement between the controller and processor in relation to processing conducted on the controller's behalf?

A. An obligation on the processor to report any personal data breach to the controller within 72 hours.
B. An obligation on both parties to report any serious personal data breach to the supervisory authority.
C. An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
D. An obligation on the processor to assist the controller in complying with the controller's obligations to notify the supervisory authority about personal data breaches.

Answer: B

NEW QUESTION 4
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 5
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 6
A German data subject was the victim of an embarrassing prank 20 years ago. A newspaper website published an article about the prank at the time, and the article is still available on the newspaper's website. Unfortunately, the prank is the top search result when a user searches on the victim's name. The data subject requests that SearchCo delist this result. SearchCo agrees, and instructs its technology team to avoid scanning or indexing the article. What else must SearchCo do?

A. Notify the newspaper that its article it is delisting the article.
B. Fully erase the URL to the content, as opposed to delist which is mainly based on data subject's name.
C. Identify other controllers who are processing the same information and inform them of the delisting request.
D. Prevent the article from being listed in search results no matter what search terms are entered into the search engine.

Answer: A

NEW QUESTION 7
In which case would a controller who has undertaken a DPIA most likely need to consult with a supervisory authority?

A. Where the DPIA identifies that personal data needs to be transferred to other countries outside of the EEA.
B. Where the DPIA identifies high risks to individuals' rights and freedoms that the controller can take steps to reduce.
C. Where the DPIA identifies that the processing being proposed collects the sensitive data of EU citizens.
D. Where the DPIA identifies risks that will require insurance for protecting its business interests.

Answer: B

NEW QUESTION 8
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 9
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 additional information must Wonderkids provide in their Privacy Statement?

A. How often promotional emails will be sent.
B. Contact information of the hosting company.
C. Technical and organizational measures to protect data.
D. The categories of recipients with whom data will be shared.

Answer: B

NEW QUESTION 10
What is the consequence if a processor makes an independent decision regarding the purposes and means of processing it carries out on behalf of a controller?

A. The controller will be liable to pay an administrative fine
B. The processor will be liable to pay compensation to affected data subjects
C. The processor will be considered to be a controller in respect of the processing concerned
D. The controller will be required to demonstrate that the unauthorized processing negatively affected oneor more of the parties involved

Answer: B

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 15
When does the GDPR provide more latitude for a company to process data beyond its original collection purpose?

A. When the data has been pseudonymized.
B. When the data is protected by technological safeguards.
C. When the data serves legitimate interest of third parties.
D. When the data subject has failed to use a provided opt-out mechanism.

Answer: C

NEW QUESTION 19
To provide evidence of GDPR compliance, a company performs an internal audit. As a result, it finds a data base, password-protected, listing all the social network followers of the client.
Regarding the domain of the controller-processor relationships, how is this situation considered?

A. Compliant with the security principle, because the data base is password-protected.
B. Non-compliant, because the storage of the data exceeds the tasks contractually authorized by the controller.
C. Not applicable, because the data base is password protected, and therefore is not at risk of identifying any data subject.
D. Compliant with the storage limitation principle, so long as the internal auditor permanently deletes the data base.

Answer: B

NEW QUESTION 22
Which change was introduced by the 2009 amendments to the e-Privacy Directive 2002/58/EC?

A. A voluntary notification for personal data breaches applicable to all data controllers.
B. A voluntary notification for personal data breaches applicable to electronic communication providers.
C. A mandatory notification for personal data breaches applicable to all data controllers.
D. A mandatory notification for personal data breaches applicable to electronic communication providers.

Answer: D

NEW QUESTION 25
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 adopts the We-Track-U pilot plan, why is it likely to be subject to the territorial scope of the GDPR?

A. Its plan would be in the context of the establishment of a controller in the Union.
B. It would be offering goods or services to data subjects in the Union.
C. It is engaging in commercial activities conducted in the Union.
D. It is monitoring the behavior of data subjects in the Union.

Answer: D

NEW QUESTION 27
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 29
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 32
What is a reason the European Court of Justice declared the Data Retention Directive invalid in 2014?

A. The requirements affected individuals without exception.
B. The requirements were financially burdensome to EU businesses.
C. The requirements specified that data must be held within the EU.
D. The requirements had limitations on how national authorities could use data.

Answer: D

NEW QUESTION 33
A company is hesitating between Binding Corporate Rules and Standard Contractual Clauses as a global data transfer solution. Which of the following statements would help the company make an effective decision?

A. Binding Corporate Rules are especially recommended for small and medium companies.
B. The data exporter does not need to be located in the EU for the standard Contractual Clauses.
C. Binding Corporate Rules provide a global solution for all the entities of a company that are bound by the intra-group agreement.
D. The company will need the prior authorization of all EU data protection authorities for concluding Standard Contractual Clauses.

Answer: C

NEW QUESTION 37
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 40
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 44
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 47
Article 5(1)(b) of the GDPR states that personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.” Based on Article 5(1)(b),
what is the impact of a member state’s interpretation of the word “incompatible”?

A. It dictates the level of security a processor must follow when using and storing personal data for two different purposes.
B. It guides the courts on the severity of the consequences for those who are convicted of the intentional misuse of personal data.
C. It sets the standard for the level of detail a controller must record when documenting the purpose for collecting personal data.
D. It indicates the degree of flexibility a controller has in using personal data in ways that may vary from its original intended purpose.

Answer: A

NEW QUESTION 48
Read the following steps:
- Discover which employees are accessing cloud services and from which devices and apps Lock down the data in those apps and devices
- Monitor and analyze the apps and devices for compliance
- Manage application life cycles
- Monitor data sharing

An organization should perform these steps to do which of the following?

A. Pursue a GDPR-compliant Privacy by Design process.
B. Institute a GDPR-compliant employee monitoring process.
C. Maintain a secure Bring Your Own Device (BYOD) program.

D. Ensure cloud vendors are complying with internal data use policies.

Answer: C

NEW QUESTION 52
Why is advisable to avoid consent as a legal basis for an employer to process employee data?

A. Employee data can only be processed if there is an approval from the data protection officer.
B. Consent may not be valid if the employee feels compelled to provide it.
C. An employer might have difficulty obtaining consent from every employee.
D. Data protection laws do not apply to processing of employee data.

Answer: A

NEW QUESTION 53
Select the answer below that accurately completes the following: “The right to compensation and liability under the GDPR…

A. …provides for an exemption from liability if the data controller (or data processor) proves that it is not in any way responsible for the event giving rise to the damage.”
B. …precludes any subsequent recourse proceedings against other controllers or processors involved in the same processing.”
C. ...can only be exercised against the data controller, even if a data processor was involved in the same processing.”
D. …is limited to a maximum amount of EUR 20 million per event of damage or loss.”

Answer: B

NEW QUESTION 55
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 Beak 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.
In preparing the company for its impending lawsuit, Alice’s instruction to the company’s IT Department violated Article 5 of the GDPR because the company failed to first do what?

A. Send out consent forms to all of its employees.
B. Minimize the amount of data collected for the lawsuit.
C. Inform all of its employees about the lawsuit.
D. Encrypt the data from all of its employees.

Answer: B

NEW QUESTION 56
When does the European Data Protection Board (EDPB) recommend reevaluating whether a transfer tool is effectively providing a level of personal data protection that is in compliance with the European Union (EU) level?

A. After a personal data breach.
B. Every three (3) years.
C. On an ongoing basis.
D. Every year.

Answer: C

NEW QUESTION 58
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 62
Which judicial body makes decisions on actions taken by individuals wishing to enforce their rights under EU law?

A. Court of Auditors
B. Court of Justice of European Union
C. European Court of Human Rights
D. European Data Protection Board

Answer: B

NEW QUESTION 66
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 69
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 71
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 73
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 78
In which of the following cases, cited as an example by a WP29 guidance, would conducting a single data protection impact assessment to address multiple processing operations be allowed?

A. A medical organization that wants to begin genetic testing to support earlier research for which they have performed a DPIA.
B. A data controller who plans to use a new technology product that has already undergone a DPIA by the product's provider.
C. A marketing team that wants to collect mailing addresses of customers for whom they already have email addresses.
D. A railway operator who plans to evaluate the same video surveillance in all the train stations of his company.

Answer: D

NEW QUESTION 81
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 Beak 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 82
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 suchas 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 87
SCENARIO
Please use the following to answer the next question:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated
speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
Why is this company obligated to comply with the GDPR?

A. The company has offices in the EU.
B. The company employs staff in the EU.
C. The company's data center is located in a country outside the EU.
D. The company's products are marketed directly to EU customers.

Answer: D

NEW QUESTION 91
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 94
What are the obligations of a processor that engages a sub-processor?

A. The processor must give the controller prior written notice and perform a preliminary audit of the sub- processor.
B. The processor must obtain the controller's specific written authorization and provide annual reports on the sub-processor's performance.
C. The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.
D. The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.

Answer: C

NEW QUESTION 95
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 98
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 100
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.
In which of the following situations would ABC Hotel Chain and XYZ Travel Agency NOT have to honor Mike's data access request?

A. The request is to obtain access and correct inaccurate personal data in his profile.
B. The request is to obtain access and information about the purpose of processing his personal data.
C. The request is to obtain access and erasure of his personal data while keeping his rewards membership.
D. The request is to obtain access and the categories of recipients who have received his personal data to process his rewards membership.

Answer: C

NEW QUESTION 103
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.
JaphSoft's use of pseudonymization is NOT in compliance with the CDPR because?

A. JaphSoft failed to first anonymize the personal data.
B. JaphSoft pseudonymized all the data instead of deleting what it no longer needed.
C. JaphSoft was in possession of information that could be used to identify data subjects.
D. JaphSoft failed to keep personally identifiable information in a separate database.

Answer: B

NEW QUESTION 106
Which of the following would require designating a data protection officer?

A. Processing is carried out by an organization employing 250 persons or more.
B. Processing is carried out for the purpose of providing for-profit goods or services to individuals in the EU.
C. The core activities of the controller or processor consist of processing operations of financial information or information relating to children.
D. The core activities of the controller or processor consist of processing operations that require systematic monitoring of data subjects on a large scale.

Answer: D

NEW QUESTION 107
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 109
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 112
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 117
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-C raze 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 120
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 124
SCENARIO
Please use the following to answer the next question:
Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.
After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.
Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.
Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.
Assuming that multiple EVETFIT branches across several EU countries are acting as separate data
controllers, and that each of those branches were responsible for mishandling Javier's request, how may Javier proceed in order to seek compensation?

A. He will have to sue the EVETFIT's head office in France, where EVETFIT has its main establishment.
B. He will be able to sue any one of the relevant EVETFIT branches, as each one may be held liable for the entire damage.
C. He will have to sue each EVETFIT branch so that each branch provides proportionate compensation commensurate with its contribution to the damage or distress suffered by Javier.
D. He will be able to apply to the European Data Protection Board in order to determine which particular EVETFIT branch is liable for damages, based on the decision that was made by the board.

Answer: A

NEW QUESTION 126
SCENARIO
Please use the following to answer the next question:
Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.
After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.
Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.
Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.
Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?

A. Submit a draft decision to other supervisory authorities for their opinion.
B. Request that the other supervisory authorities provide the lead authority with a draft decision for its consideration.
C. Submit a draft decision directly to the Commission to ensure the effectiveness of the consistency mechanism.
D. Request that members of the seconding supervisory authority and the host supervisory authority co-draft a decision.

Answer: B

NEW QUESTION 129
Which of the following is an example of direct marketing that would be subject to European data protection laws?

A. An updated privacy notice sent to an individual's personal email address.
B. A charity fundraising event notice sent to an individual at her business address.
C. A service outage notification provided to an individual by recorded telephone message.
D. A revision of contract terms conveyed to an individual by SMS from a marketing organization.

Answer: B

NEW QUESTION 134
SCENARIO
Please use the following to answer the next question:
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:

- Name
- Address
- Date of Birth
- Payroll number
- National Insurance number
- Sick pay entitlement
- Maternity/paternity pay entitlement
- Holiday entitlement
- Pension and benefits contributions
- Trade union contributions

Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B. This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she notifies all affected employees.
The GDPR requires sufficient guarantees of a company's ability to implement adequate technical and organizational measures. What would be the most realistic way that Company B could have fulfilled this requirement?

A. Hiring companies whose measures are consistent with recommendations of accrediting bodies.
B. Requesting advice and technical support from Company A's IT team.
C. Avoiding the use of another company's data to improve their own services.
D. Vetting companies' measures with the appropriate supervisory authority.

Answer: A

NEW QUESTION 135
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 137
A worker in a European Union (EU) member state has ceased his employment with a company. What should the employer most likely do in regard to the worker's personal data?

A. Destroy sensitive information and store the rest per applicable data protection rules.
B. Store all of the data in case the departing worker makes a subject access request.
C. Securely store the data that is required to be kept under local law.
D. Provide the employee the reasons for retaining the data.

Answer: A

NEW QUESTION 138
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 142
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 144
When assessing the level of risk created by a data breach, which of the following would NOT have to be taken into consideration?

A. The ease of identification of individuals.
B. The size of any data processor involved.
C. The special characteristics of the data controller.
D. The nature, sensitivity and volume of personal data.

Answer: B

NEW QUESTION 148
Pursuant to Article 4(5) of the GDPR, data is considered "pseudonymized" if?

A. It cannot be attributed to a data subject without the use of additional information.
B. It cannot be attributed to a person under any circumstances.
C. It can only be attributed to a person by the controller.
D. It can only be attributed to a person by a third party.

Answer: A

NEW QUESTION 153
What term BEST describes the European model for data protection?

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

Answer: A

NEW QUESTION 155
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 156
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 159
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
Which marketing-related activity is least likely to be covered by the provisions of Privacy and Electronic Communications Regulations (Directive 2002/58/EC)?

A. Advertisements passively displayed on a website.
B. The use of cookies to collect data about an individual.
C. A text message to individuals from a company offering concert tickets for sale.
D. An email from a retail outlet promoting a sale to one of their previous customer.

Answer: A

NEW QUESTION 168
For which of the following operations would an employer most likely be justified in requesting the data subject's consent?

A. Posting an employee's bicycle race photo on the company's social media.
B. Processing an employee's health certificate in order to provide sick leave.
C. Operating a CCTV system on company premises.
D. Assessing a potential employee's job application.

Answer: A

NEW QUESTION 170
What is true if an employee makes an access request to his employer for any personal data held about him?

A. The employer can automatically decline the request if it contains personal data about a third person.
B. The employer can decline the request if the information is only held electronically.
C. The employer must supply all the information held about the employee.
D. The employer must supply any information held about an employee unless an exemption applies.

Answer: D

NEW QUESTION 175
How is the retention of communications traffic data for law enforcement purposes addressed by European data protection law?

A. The ePrivacy Directive allows individual EU member states to engage in such data retention.
B. The ePrivacy Directive harmonizes EU member states' rules concerning such data retention.
C. The Data Retention Directive's annulment makes such data retention now permissible.
D. The GDPR allows the retention of such data for the prevention, investigation, detection or prosecution of criminal offences only.

Answer: D

NEW QUESTION 178
A Spanish electricity customer calls her local supplier with Questions: about the company's upcoming merger. Specifically, the customer wants to know the recipients to whom her personal data will be disclosed once the merger is final. According to Article 13 of the GDPR, what must the company do before providing the customer with the requested information?

A. Verify that the request is applicable to the data collected before the GDPR entered into force.
B. Verify that the purpose of the request from the customer is in line with the GDPR.
C. Verify that the personal data has not already been sent to the customer.
D. Verify that the identity of the customer can be proven by other means.

Answer: A

NEW QUESTION 179
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 181
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan
to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
With regard to TripBliss Inc.'s use of website cookies, which of the following statements is correct?

A. Because not all of the cookies are strictly necessary to enable the use of a service requested from TripBliss Inc., consent requirements apply to their use of cookies.
B. Because of the categories of data involved, explicit consent for the use of cookies must be obtained separately from customers.
C. Because Techiva will receive only aggregate statistics of data collected from the cookies, no additional consent is necessary.
D. Because the use of cookies involves the potential for location tracking, explicit consent must be obtained from customers.

Answer: B

NEW QUESTION 185
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 190
An unforeseen power outage results in company Z's lack of access to customer data for six hours. According to article 32 of the GDPR, this is considered a breach. Based on the WP 29's February, 2018 guidance, company Z should do which of the following?

A. Notify affected individuals that their data was unavailable for a period of time.
B. Document the loss of availability to demonstrate accountability
C. Notify the supervisory authority about the loss of availability
D. Conduct a thorough audit of all security systems

Answer: C

NEW QUESTION 195
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 200
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 202
According to the GDPR, how is pseudonymous personal data defined?

A. Data that can no longer be attributed to a specific data subject without the use of additional information kept separately.
B. Data that can no longer be attributed to a specific data subject, with no possibility of re-identifying the data.
C. Data that has been rendered anonymous in such a manner that the data subject is no longer identifiable.
D. Data that has been encrypted or is subject to other technical safeguards.

Answer: A

NEW QUESTION 206
Under the Data Protection Law Enforcement Directive of the EU, a government can carry out covert investigations involving personal data, as long it is set forth by law and constitutes a measure that is both necessary and what?

A. Prudent.
B. Important.
C. Proportionate.
D. DPA-approved.

Answer: C

NEW QUESTION 209
SCENARIO
Please use the following to answer the next question:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated
speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
What presents the BIGGEST potential privacy issue with the company's practices?

A. The NFC portal can read any data stored in the action figures
B. The information about the data processing involved has not been specified
C. The cloud service provider is in a country that has not been deemed adequate
D. The RFID tag in the action figures has the potential for misuse because of the toy's evolving capabilities

Answer: B

NEW QUESTION 210
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 212
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.
In addition to notifying employees about the purpose of the monitoring, the potential uses of their data and their privacy rights, what information should Building Block have provided them before implementing the security measures?

A. Information about what is specified in the employment contract.
B. Information about who employees should contact with any queries.
C. Information about how providing consent could affect them as employees.
D. Information about how the measures are in the best interests of the company.

Answer: A

NEW QUESTION 217
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 222
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 is the time period in which Mike should receive a response to his request?

A. Not more than one month of receipt of Mike's request.
B. Not more than two months after verifying Mike's identity.
C. When all the information about Mike has been collected.
D. Not more than thirty days after submission of Mike's request.

Answer: D

NEW QUESTION 225
According to the E-Commerce Directive 2000/31/EC, where is the place of "establishment" for a company providing services via an Internet website confirmed by the GDPR?

A. Where the technology supporting the website is located
B. Where the website is accessed
C. Where the decisions about processing are made
D. Where the customer's Internet service provider is located

Answer: D

NEW QUESTION 228
Under Article 9 of the GDPR, which of the following categories of data is NOT expressly prohibited from data processing?

A. Personal data revealing ethnic origin.
B. Personal data revealing genetic data.
C. Personal data revealing financial data.
D. Personal data revealing trade union membership.

Answer: C

NEW QUESTION 231
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 233
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-Heaith 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 235
Which mechanism, new to the GDPR, now allows for the possibility of personal data transfers to third countries under Article 42?

A. Approved certifications.
B. Binding corporate rules.
C. Law enforcement requests.
D. Standard contractual clauses.

Answer: A

NEW QUESTION 236
A company is located in a country NOT considered by the European Union (EU) to have an adequate level of data protection. Which of the following is an obligation of the company if it imports personal data from another organization in the European Economic Area (EEA) under standard contractual clauses?

A. Submit the contract to its own government authority.
B. Ensure that notice is given to and consent is obtained from data subjects.
C. Supply any information requested by a data protection authority (DPA) within 30 days.
D. Ensure that local laws do not impede the company from meeting its contractual obligations.

Answer: A

NEW QUESTION 240
Tanya is the Data Protection Officer for Curtains Inc., a GDPR data controller. She has recommended that the company encrypt all personal data at rest. Which GDPR principle is she following?

A. Accuracy
B. Storage Limitation
C. Integrity and confidentiality
D. Lawfulness, fairness and transparency

Answer: C

NEW QUESTION 241
SCENARIO
Please use the following to answer the next question:
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B.
Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:

- Name
- Address
- Date of Birth
- Payroll number
- National Insurance number
- Sick pay entitlement
- Maternity/paternity pay entitlement
- Holiday entitlement
- Pension and benefits contributions
- Trade union contributions

Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B. This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to
Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she notifies all affected employees.
Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?

A. Their omission of data protection provisions in their contract with Company C.
B. Their failure to provide sufficient security safeguards to Company A's data.
C. Their engagement of Company C to improve their payroll service.
D. Their decision to operate without a data protection officer.

Answer: C

NEW QUESTION 243
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.
Based on the scenario, what is the main reason that Brady should be concerned with Hermes Designs' handling of customer personal data?

A. The data is sensitive.
B. The data is uncategorized.
C. The data is being used for a new purpose.
D. The data is being processed via a new means.

Answer: D

NEW QUESTION 245
SCENARIO
Please use the following to answer the next question:
Dynaroux Fashion ('Dynaroux') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Ronan 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, Jonas, the CEO, tells Ronan 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. Ronan tells the CEO that: (a) the potential risks of such activities means that
Dynaroux 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, Dynaroux may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jonas tells Ronan that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Dynaroux's business plan and associated processing activities.
Which of the following facts about Dynaroux would trigger a data protection impact assessment under the GDPR?

A. The company will be undertaking processing activities involving sensitive data categories such as financial and children's data.
B. The company employs approximately 650 people and will therefore be carrying out extensive processing activities.
C. The company plans to undertake profiling of its customers through analysis of their purchasing patterns.
D. The company intends to shift their business model to rely more heavily on online shopping.

Answer: C

NEW QUESTION 248
An organization conducts body temperature checks as a part of COVID-19 monitoring. Body temperature is measured manually and is not followed by registration, documentation or other processing of an individual's personal data.
Which of the following best explain why this practice would NOT be subject to the GDPR?

A. Body temperature is not considered personal data.
B. The practice does not involve completion by automated means.
C. Body temperature is considered pseudonymous data.
D. The practice is for the purpose of alleviating extreme risks to public health.

Answer: B

NEW QUESTION 253

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 255
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CIPP-E Practice Exam Features:

* CIPP-E Questions and Answers Updated Frequently

* CIPP-E Practice Questions Verified by Expert Senior Certified Staff

* CIPP-E Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CIPP-E Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year