

IAPP

Exam Questions CIPP-E

Certified Information Privacy Professional/Europe (CIPP/E)



NEW QUESTION 1

Article 29 Working Party has emphasized that the GDPR forbids “forum shopping”, which occurs when companies do what?

- A. Choose the data protection officer that is most sympathetic to their business concerns.
- B. Designate their main establishment in member state with the most flexible practices.
- C. File appeals of infringement judgments with more than one EU institution simultaneously.
- D. Select third-party processors on the basis of cost rather than quality of privacy protection.

Answer: B

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

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 4

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

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

Answer: D

NEW QUESTION 5

SCENARIO

Please use the following to answer the next QUESTION NO:

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

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

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

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

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

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

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

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

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

Answer: B

NEW QUESTION 6

Which of the following entities would most likely be exempt from complying with the GDPR?

- A. A South American company that regularly collects European customers' personal data.
- B. A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state.
- C. A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers.
- D. A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

Answer: C

NEW QUESTION 7

An online company's privacy practices vary due to the fact that it offers a wide variety of services. How could it best address the concern that explaining them all would make the policies incomprehensible?

- A. Use a layered privacy notice on its website and in its email communications.
- B. Identify uses of data in a privacy notice mailed to the data subject.
- C. Provide only general information about its processing activities and offer a toll-free number for more information.
- D. Place a banner on its website stipulating that visitors agree to its privacy policy and terms of use by visiting the site.

Answer: B

NEW QUESTION 8

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 9

Which of the following is the weakest lawful basis for processing employee personal data?

- A. Processing based on fulfilling an employment contract.
- B. Processing based on employee consent.
- C. Processing based on legitimate interests.
- D. Processing based on legal obligation.

Answer: B

NEW QUESTION 10

Under the GDPR, which of the following is true in regard to adequacy decisions involving cross-border transfers?

- A. The European Commission can adopt an adequacy decision for individual companies.
- B. The European Commission can adopt, repeal or amend an existing adequacy decision.
- C. EU member states are vested with the power to accept or reject a European Commission adequacy decision.
- D. To be considered as adequate, third countries must implement the EU General Data Protection Regulation into their national legislation.

Answer: A

NEW QUESTION 10

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

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

Answer: A

NEW QUESTION 11

SCENARIO

Please use the following to answer the next question:

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

Registration Form

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

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

provider, Stratculous. (Read more about Stratculous here.)

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

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

- > First name:
- > Surname:
- > Year of birth:
- > Email:
- > Physical Address (optional*):
- > Health status:

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

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

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

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

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

Answer: D

NEW QUESTION 15

What obligation does a data controller or processor have after appointing a data protection officer?

- A. To ensure that the data protection officer receives sufficient instructions regarding the exercise of his or her defined tasks.
- B. To provide resources necessary to carry out the defined tasks of the data protection officer and to maintain his or her expert knowledge.
- C. To ensure that the data protection officer acts as the sole point of contact for individuals' Questions: about their personal data.
- D. To submit for approval to the data protection officer a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.

Answer: D

NEW QUESTION 16

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

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

Answer: B

NEW QUESTION 17

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.

For what reason would JaphSoft be considered a controller under the GDPR?

- A. It determines how long to retain the personal data collected.
- B. It has been provided access to personal data in the MarketIQ database.
- C. It uses personal data to improve its products and services for its client-base through machine learning.
- D. It makes decisions regarding the technical and organizational measures necessary to protect the personal data.

Answer: D

NEW QUESTION 20

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 25

Article 58 of the GDPR describes the power of supervisory authorities. Which of the following is NOT among those granted?

- A. Legislative powers.
- B. Corrective powers.
- C. Investigatory powers.
- D. Authorization and advisory powers.

Answer: D

NEW QUESTION 27

Under which of the following conditions does the General Data Protection Regulation NOT apply to the processing of personal data?

- A. When the personal data is processed only in non-electronic form
- B. When the personal data is collected and then pseudonymised by the controller
- C. When the personal data is held by the controller but not processed for further purposes
- D. When the personal data is processed by an individual only for their household activities

Answer: B

NEW QUESTION 31

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 32

An employee of company ABCD has just noticed a memory stick containing records of client data, including their names, addresses and full contact details has disappeared. The data on the stick is unencrypted and in clear text. It is uncertain what has happened to the stick at this stage, but it likely was lost during the travel of an employee. What should the company do?

- A. Notify as soon as possible the data protection supervisory authority that a data breach may have taken place.
- B. Launch an investigation and if nothing is found within one month, notify the data protection supervisory authority.
- C. Invoke the “disproportionate effort” exception under Article 33 to postpone notifying data subjects until more information can be gathered.
- D. Immediately notify all the customers of the company that their information has been accessed by an unauthorized person.

Answer: A

NEW QUESTION 37

How does the GDPR now define “processing”?

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

Answer: A

NEW QUESTION 41

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.

What is the nature of BHealthy and Natural Insight's relationship?

- A. Natural Insight is BHealthy's processor because the companies entered into data processing terms.
- B. Natural Insight is BHealthy's processor because BHealthy is sharing its customer information with Natural Insight.
- C. Natural Insight is the controller because it determines the security measures to implement to protect data it processes; BHealthy is a co-controller because it engaged Natural Insight to determine pricing for the new sunscreens.
- D. Natural Insight is a controller because it is separately determine the purpose of processing when it uses BHealthy's customer information to improve its machine learning algorithms.

Answer: A

NEW QUESTION 45

Under the GDPR, who would be LEAST likely to be allowed to engage in the collection, use, and disclosure of a data subject's sensitive medical information without the data subject's knowledge or consent?

- A. A member of the judiciary involved in adjudicating a legal dispute involving the data subject and concerning the health of the data subject.
- B. A public authority responsible for public health, where the sharing of such information is considered necessary for the protection of the general populace.
- C. A health professional involved in the medical care for the data subject, where the data subject's life hinges on the timely dissemination of such information.
- D. A journalist writing an article relating to the medical condition in QUESTION, who believes that the publication of such information is in the public interest.

Answer: B

NEW QUESTION 50

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

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 51

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 is the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U?

- A. Conduct analysis only on anonymized personal data.
- B. Conduct analysis only on pseudonymized personal data.
- C. Delete all data collected prior to May 2018 after conducting the trend analysis.
- D. Procure a third party to conduct the analysis and delete the data from Market4U's systems.

Answer: A

NEW QUESTION 52

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

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

Answer: A

NEW QUESTION 54

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 59

In which of the following cases would an organization MOST LIKELY be required to follow both ePrivacy and data protection rules?

- A. When creating an untargeted pop-up ad on a website.
- B. When calling a potential customer to notify her of an upcoming product sale.
- C. When emailing a customer to announce that his recent order should arrive earlier than expected.
- D. When paying a search engine company to give prominence to certain products and services within specific search results.

Answer: A

NEW QUESTION 61

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 65

Which institution has the power to adopt findings that confirm the adequacy of the data protection level in a non-EU country?

- A. The European Parliament
- B. The European Commission
- C. The Article 29 Working Party
- D. The European Council

Answer: B

NEW QUESTION 68

After leaving the EU under the terms of Brexit, the United Kingdom will seek an adequacy determination. What is the reason for this?

- A. The Insurance Commissioner determined that an adequacy determination is required by the Data Protection Act.
- B. Adequacy determinations automatically lapse when a Member State leaves the EU.

- C. The UK is now a third country because it's no longer subject to the GDPR.
- D. The UK is less trustworthy now that its not part of the Union.

Answer: C

NEW QUESTION 73

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.

In light of the requirements of Article 32 of the GDPR (related to the Security of Processing), which practice should the company institute?

- A. Encrypt the data in transit over the wireless Bluetooth connection.
- B. Include dual-factor authentication before each use by a child in order to ensure a minimum amount of security.
- C. Include three-factor authentication before each use by a child in order to ensure the best level of security possible.
- D. Insert contractual clauses into the contract between the toy manufacturer and the cloud service provider, since South Africa is outside the European Union.

Answer: A

NEW QUESTION 78

SCENARIO

Please use the following to answer the next question:

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

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

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

Which of the following is T-Craze's lead supervisory authority?

- A. Germany, because that is where T-Craze is headquartered.
- B. France, because that is where T-Craze conducts processing of personal information.
- C. Spain, because that is T-Craze's primary market based on its marketing campaigns.
- D. T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.

Answer: C

NEW QUESTION 80

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

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

Answer: C

NEW QUESTION 84

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 87

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 88

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

Answer: D

NEW QUESTION 89

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 90

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

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

Answer: B

NEW QUESTION 95

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

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

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

Answer: A

NEW QUESTION 97

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 100

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

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

Answer: B

NEW QUESTION 102

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 104

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 109

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 111

What should a controller do after a data subject opts out of a direct marketing activity?

- A. Without exception, securely delete all personal data relating to the data subject.
- B. Without undue delay, provide information to the data subject on the action that will be taken.
- C. Refrain from processing personal data relating to the data subject for the relevant type of communication.
- D. Take reasonable steps to inform third-party recipients that the data subject's personal data should be deleted and no longer processed.

Answer: C

NEW QUESTION 116

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

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

Answer: B

NEW QUESTION 121

Under the GDPR, where personal data is not obtained directly from the data subject, a controller is exempt from directly providing information about processing to the data subject if?

- A. The data subject already has information regarding how his data will be used
- B. The provision of such information to the data subject would be too problematic
- C. Third-party data would be disclosed by providing such information to the data subject
- D. The processing of the data subject's data is protected by appropriate technical measures

Answer: A

NEW QUESTION 125

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 129

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 133

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 134

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

Answer: D

NEW QUESTION 139

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 current trends in European privacy practices, which aspect of Brady Box' Online Behavioral Advertising (OBA) is most likely to be insufficient if the company becomes established in Europe?

- A. The lack of the option to opt in.
- B. The level of security within the website.
- C. The contract with the third-party advertising network.
- D. The need to have the contents of the advertising approved.

Answer: A

NEW QUESTION 142

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 EVERFIT 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 EVERFIT 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 146

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 151

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 152

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

Answer: C

NEW QUESTION 155

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 156

When would a data subject NOT be able to exercise the right to portability?

- A. When the processing is necessary to perform a task in the exercise of authority vested in the controller.
- B. When the processing is carried out pursuant to a contract with the data subject.
- C. When the data was supplied to the controller by the data subject.
- D. When the processing is based on consent.

Answer: A

NEW QUESTION 161

The GDPR forbids the practice of "forum shopping", which occurs when companies do what?

- A. Choose the data protection officer that is most sympathetic to their business concerns.
- B. Designate their main establishment in member state with the most flexible practices.
- C. File appeals of infringement judgments with more than one EU institution simultaneously.
- D. Select third-party processors on the basis of cost rather than quality of privacy protection.

Answer: B

NEW QUESTION 164

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 165

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 169

Under Article 80(1) of the GDPR, individuals can elect to be represented by not-for-profit organizations in a privacy group litigation or class action. These organizations are commonly known as?

- A. Law firm organizations.
- B. Civil society organizations.
- C. Human rights organizations.
- D. Constitutional rights organizations.

Answer: A

NEW QUESTION 171

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

- A. A prior opt-in consent for consumers unless they are already customers.
- B. A pre-checked box stating that the consumer agrees to receive email marketing.
- C. A notice that the consumer's email address will be used for marketing purposes.
- D. No prior permission required, but an opt-out requirement on all emails sent to consumers.

Answer: A

NEW QUESTION 175

Company X has entrusted the processing of their payroll data to Provider Y. Provider Y stores this encrypted data on its server. The IT department of Provider Y finds out that someone managed to hack into the system and take a copy of the data from its server. In this scenario, whom does Provider Y have the obligation to notify?

- A. The public
- B. Company X
- C. Law enforcement

D. The supervisory authority

Answer: C

NEW QUESTION 176

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 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.

Under the GDPR, what are Natural Insight's security obligations with respect to the customer information it received from BHealthy?

- A. Appropriate security that takes into account the industry practices for protecting customer contact information and purchase history.
- B. Only the security measures assessed by BHealthy prior to entering into the data processing contract.
- C. Absolute security since BHealthy is sharing personal data, including purchase history, with Natural Insight.
- D. The level of security that a reasonable data subject whose data is processed would expect in relation to the data subject's purchase history.

Answer: A

NEW QUESTION 182

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 187

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

The data transfer mechanism that Alice drafted violates the GDPR because the company did not first get approval from?

- A. The Court of Justice of the European Union.
- B. The European Data Protection Board.
- C. The Data Protection Authority.
- D. The European Commission.

Answer: C

NEW QUESTION 188

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

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

Answer: D

NEW QUESTION 189

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 190

Which of the following describes a mandatory requirement for a group of undertakings that wants to appoint a single data protection officer?

- A. The group of undertakings must obtain approval from a supervisory authority.
- B. The group of undertakings must be comprised of organizations of similar sizes and functions.
- C. The data protection officer must be located in the country where the data controller has its main establishment.
- D. The data protection officer must be easily accessible from each establishment where the undertakings are located.

Answer: D

NEW QUESTION 195

Which of the following would most likely NOT be covered by the definition of "personal data" under the GDPR?

- A. The payment card number of a Dutch citizen
- B. The U.
- C. social security number of an American citizen living in France
- D. The unlinked aggregated data used for statistical purposes by an Italian company
- E. The identification number of a German candidate for a professional examination in Germany

Answer: D

NEW QUESTION 198

Which of the following Convention 108+ principles, as amended in 2018, is NOT consistent with a principle found in the GDPR?

- A. The obligation of companies to declare data breaches.
- B. The requirement to demonstrate compliance to a supervisory authority.
- C. The necessity of the bulk collection of personal data by the government.

Answer: B

NEW QUESTION 201

SCENARIO

Please use the following to answer the next question:

Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:

- Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.
- Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).
- Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees.

These records are available to former students after registering through Granchester's Alumni portal. Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.

- Under their security policy, the University encrypts all of its personal data records in transit and at rest.

In order to improve his teaching, Frank wants to investigate how his engineering students perform in relational to Department for Education expectations. He has attended one of Anna's data protection training courses and knows that he should use no more personal data than necessary to accomplish his goal. He creates a program that will only export some student data: previous schools attended, grades originally obtained, grades currently obtained and first time university attended. He wants to keep the records at the individual student level. Mindful of Anna's training, Frank runs the student numbers through an algorithm to transform them into different reference numbers. He uses the same algorithm on each occasion so that he can update each record over time.

One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR.

After receiving her email reminder, Frank informs

Anna about his performance database.

Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after

she has done some additional research.

Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.

Which of the University's records does Anna NOT have to include in her record of processing activities?

- A. Student records
- B. Staff and alumni records
- C. Frank's performance database
- D. Department for Education records

Answer: C

NEW QUESTION 206

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 211

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 213

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 215

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 220

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 225

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 228

Which sentence BEST summarizes the concepts of “fairness,” “lawfulness” and “transparency”, as expressly required by Article 5 of the GDPR?

- A. Fairness and transparency refer to the communication of key information before collecting data; lawfulness refers to compliance with government regulations.
- B. Fairness refers to limiting the amount of data collected from individuals; lawfulness refers to the approval of company guidelines by the state; transparency solely relates to communication of key information before collecting data.
- C. Fairness refers to the security of personal data; lawfulness and transparency refers to the analysis of ordinances to ensure they are uniformly enforced.
- D. Fairness refers to the collection of data from diverse subjects; lawfulness refers to the need for legal rules to be uniform; transparency refers to giving individuals access to their data.

Answer: A

NEW QUESTION 230

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 234

SCENARIO

Please use the following to answer the next question:

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

Registration Form

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

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

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

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

- > First name:
- > Surname:
- > Year of birth:
- > Email:
- > Physical Address (optional*):
- > Health status:

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

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

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

send automated emails with alerts regarding any problems with the M-Health app that may affect your well being. Emily sends the draft to Sam for review. Which of the following is Sam most likely to point out as the biggest problem with Emily's consent provision?

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

Answer: C

NEW QUESTION 239

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 240

Which of the following demonstrates compliance with the accountability principle found in Article 5, Section 2 of the GDPR?

- A. Anonymizing special categories of data.
- B. Conducting regular audits of the data protection program.
- C. Getting consent from the data subject for a cross border data transfer.
- D. Encrypting data in transit and at rest using strong encryption algorithms.

Answer: B

NEW QUESTION 244

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

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

Answer: C

NEW QUESTION 249

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

Ben's collection of additional data from customers created several potential issues for the company, which would most likely require what?

- A. New corporate governance and code of conduct.
- B. A data protection impact assessment.
- C. A comprehensive data inventory.
- D. Hiring a data protection officer.

Answer: A

NEW QUESTION 253

According to the GDPR, when should the processing of photographs be considered processing of special categories of personal data?

- A. When processed with the intent to publish information regarding a natural person on publicly accessible media.
- B. When processed with the intent to proceed to scientific or historical research projects.

- C. When processed with the intent to uniquely identify or authenticate a natural person.
- D. When processed with the intent to comply with a law.

Answer: C

NEW QUESTION 255

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 259

If a company is planning to use closed-circuit television (CCTV) on its premises and is concerned with GDPR compliance, it should first do all of the following EXCEPT?

- A. Notify the appropriate data protection authority.
- B. Perform a data protection impact assessment (DPIA).
- C. Create an information retention policy for those who operate the system.
- D. Ensure that safeguards are in place to prevent unauthorized access to the footage.

Answer: C

NEW QUESTION 262

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

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

Answer: B

NEW QUESTION 267

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 270

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The CIPP-E Practice Test Here](#)