

Exam Questions CIPP-E

Certified Information Privacy Professional/Europe (CIPP/E)

<https://www.2passeasy.com/dumps/CIPP-E/>



NEW QUESTION 1

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

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

Answer: D

NEW QUESTION 2

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

Answer: A

NEW QUESTION 3

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

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

Answer: C

NEW QUESTION 4

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

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

Answer: A

NEW QUESTION 5

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

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

Answer: C

NEW QUESTION 6

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

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

Answer: B

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

Data retention in the EU was underpinned by a legal framework established by the Data Retention Directive (2006/24/EC). Why is the Directive no longer part of EU law?

- A. The Directive was superseded by the EU Directive on Privacy and Electronic Communications.
- B. The Directive was superseded by the General Data Protection Regulation.
- C. The Directive was annulled by the Court of Justice of the European Union.
- D. The Directive was annulled by the European Court of Human Rights.

Answer: C

NEW QUESTION 9

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

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

Answer: D

NEW QUESTION 10

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 10

What is a reason the European Court of Justice declared the Data Retention Directive invalid in 2014?

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

Answer: D

NEW QUESTION 12

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

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

Answer: A

NEW QUESTION 13

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 14

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 17

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 21

Read the following steps:

- > Discover which employees are accessing cloud services and from which devices and apps Lock down the data in those apps and devices
- > Monitor and analyze the apps and devices for compliance
- > Manage application life cycles
- > Monitor data sharing

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

- A. Pursue a GDPR-compliant Privacy by Design process.
- B. Institute a GDPR-compliant employee monitoring process.
- C. Maintain a secure Bring Your Own Device (BYOD) program.
- D. Ensure cloud vendors are complying with internal data use policies.

Answer: C

NEW QUESTION 24

Select the answer below that accurately completes the following: “The right to compensation and liability under the GDPR...

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

Answer: B

NEW QUESTION 27

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 30

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 33

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 37

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 41

With respect to international transfers of personal data, the European Data Protection Board (EDPB) confirmed that derogations may be relied upon under what condition?

- A. If the data controller has received preapproval from a Data Protection Authority (DPA), after submitting the appropriate documents.
- B. When it has been determined that adequate protection can be performed.
- C. Only if the Data Protection Impact Assessment (DPIA) shows low risk.
- D. Only as a last resort and when interpreted restrictively.

Answer: B

NEW QUESTION 44

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

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

Answer: A

NEW QUESTION 47

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 52

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

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

Answer: A

NEW QUESTION 54

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

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

Answer: C

NEW QUESTION 59

The European Parliament jointly exercises legislative and budgetary functions with which of the following?

- A. The European Commission.
- B. The Article 29 Working Party.
- C. The Council of the European Union.
- D. The European Data Protection Board.

Answer: C

NEW QUESTION 63

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

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

Answer: B

NEW QUESTION 66

SCENARIO

Please use the following to answer the next question:

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 69

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

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

Answer: B

NEW QUESTION 74

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

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

Answer: D

NEW QUESTION 76

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

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

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

Answer: A

NEW QUESTION 77

What is true of both the General Data Protection Regulation (GDPR) and the Council of Europe Convention 108?

- A. Both govern international transfers of personal data
- B. Both govern the manual processing of personal data
- C. Both only apply to European Union countries
- D. Both require notification of processing activities to a supervisory authority

Answer: D

NEW QUESTION 80

According to the GDPR, what is the main task of a Data Protection Officer (DPO)?

- A. To create and maintain records of processing activities.
- B. To conduct Privacy Impact Assessments on behalf of the controller or processor.
- C. To monitor compliance with other local or European data protection provisions.

D. To create procedures for notification of personal data breaches to competent supervisory authorities.

Answer: B

NEW QUESTION 81

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 84

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 86

What are the obligations of a processor that engages a sub-processor?

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

Answer: C

NEW QUESTION 90

SCENARIO

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts. Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations. Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information. Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company. JaphSoft's use of pseudonymization is NOT in compliance with the CDPR because?

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

Answer: B

NEW QUESTION 95

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 97

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

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

Answer: D

NEW QUESTION 100

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 103

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 104

What is the most frequently used mechanism for legitimizing cross-border data transfer?

- A. Standard Contractual Clauses.
- B. Approved Code of Conduct.
- C. Binding Corporate Rules.
- D. Derogations.

Answer: A

NEW QUESTION 107

What term BEST describes the European model for data protection?

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

Answer: A

NEW QUESTION 111

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 116

Which of the following is NOT a role of works councils?

- A. Determining the monetary fines to be levied against employers for data breach violations of employee data.
- B. Determining whether to approve or reject certain decisions of the employer that affect employees.
- C. Determining whether employees' personal data can be processed or not.
- D. Determining what changes will affect employee working conditions.

Answer: C

NEW QUESTION 121

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 126

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 129

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 134

Which of the following is NOT an explicit right granted to data subjects under the GDPR?

- A. The right to request access to the personal data a controller holds about them.
- B. The right to request the deletion of data a controller holds about them.
- C. The right to opt-out of the sale of their personal data to third parties.
- D. The right to request restriction of processing of personal data, under certain scenarios.

Answer: A

NEW QUESTION 135

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.

When Ben had the company collect additional data from its customers, the most serious violation of the GDPR occurred because the processing of the data created what?

- A. An information security risk by copying the data into a new database.
- B. A potential legal liability and financial exposure from its customers.
- C. A significant risk to the customers' fundamental rights and freedoms.
- D. A significant risk due to the lack of an informed consent mechanism.

Answer: C

NEW QUESTION 138

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 139

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

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

Answer: D

NEW QUESTION 140

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 144

SCENARIO

Please use the following to answer the next question:

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

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

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

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

Answer: A

NEW QUESTION 148

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 150

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 151

SCENARIO

Please use the following to answer the next question:

TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.

During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan

to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.

With regard to TripBliss Inc.'s use of website cookies, which of the following statements is correct?

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

Answer: B

NEW QUESTION 154

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 156

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

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

Answer: A

NEW QUESTION 157

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

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

Answer: C

NEW QUESTION 158

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

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

Answer: B

NEW QUESTION 160

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 165

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 167

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 168

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 171

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

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

Answer: A

NEW QUESTION 174

SCENARIO

Please use the following to answer the next question:

TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.

During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.

After Leon has informed his manager, what is Techiva's legal responsibility as a processor?

- A. They must report it to TripBliss Inc.
- B. They must conduct a full systems audit.
- C. They must report it to the supervisory authority.
- D. They must inform customers who have used the website.

Answer: B

NEW QUESTION 175

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 179

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

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

Answer: C

NEW QUESTION 180

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 182

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

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

Answer: B

Explanation:

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

NEW QUESTION 187

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CIPP-E Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CIPP-E Product From:

<https://www.2passeasy.com/dumps/CIPP-E/>

Money Back Guarantee

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