

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

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 3

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 4

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 5

Please use the following to answer the next question:

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

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

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

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

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

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

Answer: C

NEW QUESTION 6

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

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

Answer: C

NEW QUESTION 7

If a company chooses to ground an international data transfer on the contractual route, which of the following is NOT a valid set of standard contractual clauses?

- A. Decision 2001/497/EC (EU controller to non-EU or EEA controller).
- B. Decision 2004/915/EC (EU controller to non-EU or EEA controller).
- C. Decision 2007/72/EC (EU processor to non-EU or EEA controller).
- D. Decision 2010/87/EU (Non-EU or EEA processor from EU controller).

Answer: B

NEW QUESTION 8

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 9

What is one major goal that the OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) all had in common but largely failed to achieve in Europe?

- A. The establishment of a list of legitimate data processing criteria
- B. The creation of legally binding data protection principles
- C. The synchronization of approaches to data protection
- D. The restriction of cross-border data flow

Answer: D

NEW QUESTION 10

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

SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

If Who-R-U adopts the We-Track-U pilot plan, why is it likely to be subject to the territorial scope of the GDPR?

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

Answer: D

NEW QUESTION 12

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 13

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 15

SCENARIO

Please use the following to answer the next question:

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

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

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

To comply with the GDPR, what should Building Block have done as a first step before implementing the SecurityScan measure?

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

Answer: C

NEW QUESTION 17

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 18

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 21

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 22

According to Article 14 of the GDPR, how long does a controller have to provide a data subject with necessary privacy information, if that subject's personal data has been obtained from other sources?

- A. As soon as possible after obtaining the personal data.
- B. As soon as possible after the first communication with the data subject.
- C. Within a reasonable period after obtaining the personal data, but no later than one month.
- D. Within a reasonable period after obtaining the personal data, but no later than eight weeks.

Answer: A

NEW QUESTION 27

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

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

Answer: D

NEW QUESTION 28

Under the GDPR, which essential pieces of information must be provided to data subjects before collecting their personal data?

- A. The authority by which the controller is collecting the data and the third parties to whom the data will be sent.
- B. The name/s of relevant government agencies involved and the steps needed for revising the data.
- C. The identity and contact details of the controller and the reasons the data is being collected.
- D. The contact information of the controller and a description of the retention policy.

Answer: C

NEW QUESTION 31

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 35

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 39

The GDPR requires controllers to supply data subjects with detailed information about the processing of their data. Where a controller obtains data directly from data subjects, which of the following items of information does NOT legally have to be supplied?

- A. The recipients or categories of recipients.
- B. The categories of personal data concerned.
- C. The rights of access, erasure, restriction, and portability.
- D. The right to lodge a complaint with a supervisory authority.

Answer: B

NEW QUESTION 44

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

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

Answer: B

NEW QUESTION 49

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 52

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 57

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

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

Answer: C

NEW QUESTION 60

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 62**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.

If TripBliss Inc. decides not to report the incident to the supervisory authority, what would be their BEST defense?

- A. The resulting obligation to notify data subjects would involve disproportionate effort.
- B. The incident resulted from the actions of a third-party that were beyond their control.
- C. The destruction of the stolen data makes any risk to the affected data subjects unlikely.
- D. The sensitivity of the categories of data involved in the incident was not substantial enough.

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 71

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

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

Answer: D

NEW QUESTION 75**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.

Anna will find that a risk analysis is NOT necessary in this situation as long as?

- A. The data subjects are no longer current students of Frank's
- B. The processing will not negatively affect the rights of the data subjects
- C. The algorithms that Frank uses for the processing are technologically sound
- D. The data subjects gave their unambiguous consent for the original processing

Answer: D

NEW QUESTION 78

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

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

Answer: D

NEW QUESTION 80

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 85

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 90

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 92

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 93

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 98

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 101

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 104

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 106

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

- A. Inform the subjects about the collection
- B. Provide a public notice regarding the data
- C. Upgrade security to match that of the source
- D. Update the data within a reasonable timeframe

Answer: A

NEW QUESTION 111

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 113

What must a data controller do in order to make personal data pseudonymous?

- A. Separately hold any information that would allow linking the data to the data subject.
- B. Encrypt the data in order to prevent any unauthorized access or modification.
- C. Remove all indirect data identifiers and dispose of them securely.
- D. Use the data only in aggregated form for research purposes.

Answer: A

NEW QUESTION 115

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 117

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

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

Answer: B

NEW QUESTION 119

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 124

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 127

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 131

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 133

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

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

Answer: C

NEW QUESTION 135

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 140

SCENARIO

Please use the following to answer the next question:

Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.

Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.

Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.

Assuming that multiple EVETFIT branches across several EU countries are acting as separate data controllers, and that each of those branches were responsible for mishandling Javier's request, how may Javier proceed in order to seek compensation?

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

Answer: A

NEW QUESTION 143

SCENARIO

Please use the following to answer the next question:

Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.

Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.

Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.

Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?

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

Answer: B

NEW QUESTION 144

Which EU institution is vested with the competence to propose new data protection legislation on its own initiative?

- A. The European Council
- B. The European Parliament
- C. The European Commission
- D. The Council of the European Union

Answer: D

NEW QUESTION 145

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 150

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 152

Which of the following countries will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary?

- A. Greece
- B. Norway
- C. Australia
- D. Switzerland

Answer: D

NEW QUESTION 157

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

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

Answer: B

NEW QUESTION 159

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 162

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 164

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 167

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 169

The Planet 49 CJEU Judgement applies to?

- A. Cookies used only by third parties.
- B. Cookies that are deemed technically necessary.
- C. Cookies regardless of whether the data accessed is personal or not.
- D. Cookies where the data accessed is considered as personal data only.

Answer: C

NEW QUESTION 170

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 171

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

- A. Posting an employee's bicycle race photo on the company's social media.
- B. Processing an employee's health certificate in order to provide sick leave.

- C. Operating a CCTV system on company premises.
- D. Assessing a potential employee's job application.

Answer: A

NEW QUESTION 174

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

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

Answer: D

NEW QUESTION 179

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 181

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 182

A U.S. company's website sells widgets. Which of the following factors would NOT in itself subject the company to the GDPR?

- A. The widgets are offered in EU and priced in euro.
- B. The website is in English and French, and is accessible in France.
- C. An affiliate office is located in France but the processing is in the U.S.
- D. The website places cookies to monitor the EU website user behavior.

Answer: B

NEW QUESTION 185

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 186

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 187

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 190

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 193

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 198

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 203

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

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

Answer: C

NEW QUESTION 204

SCENARIO

Please use the following to answer the next question:

You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.

The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.

When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.

In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.

What presents the BIGGEST potential privacy issue with the company's practices?

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

Answer: B

NEW QUESTION 209

When is data sharing agreement MOST likely to be needed?

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

Answer: B

NEW QUESTION 212

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 215

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 217

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 222

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

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

Answer: D

NEW QUESTION 226

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 227

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 232

There are three domains of security covered by Article 32 of the GDPR that apply to both the controller and the processor. These include all of the following EXCEPT?

- A. Consent management and withdrawal.
- B. Incident detection and response.
- C. Preventative security.
- D. Remedial security.

Answer: A

NEW QUESTION 234

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 239

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 243

SCENARIO

Please use the following to answer the next question:

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

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

In an aggressive bid to build revenue growth, Jonas, the CEO, tells Ronan that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Ronan tells the CEO that: (a) the potential risks of such activities means that

Dynaroux needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate

protection measures, Dynaroux may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

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

Which of the following facts about Dynaroux would trigger a data protection impact assessment under the GDPR?

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

Answer: C

NEW QUESTION 244

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 246

.....

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](#)