IAPP

Exam Questions CIPP-E

Certified Information Privacy Professional/Europe (CIPP/E)

NEW QUESTION 1
If a French controller has a car-sharing app available only in Morocco, Algeria and Tunisia, but the data processing activities are carried out by the appointed processor in Spain, the GDPR will apply to the processing of the personal data so long as?

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

Answer: D

NEW QUESTION 2
To which of the following parties does the territorial scope of the GDPR NOT apply?

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

Answer: A

NEW QUESTION 3
In which case would a controller who has undertaken a DPIA most likely need to consult with a supervisory authority?

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

Answer: B

NEW QUESTION 4
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.
Before Anna determines whether Frank's performance database is permissible, what additional information does she need?

A. More information about Frank's data protection training.
B. More information about the extent of the information loss.
C. More information about the algorithm Frank used to mask student numbers.
D. More information about what students have been told and how the research will be used.

Answer: D

NEW QUESTION 5
Which sentence best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

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

Answer: C

NEW QUESTION 6
According to Article 84 of the GDPR, the rules on penalties applicable to infringements shall be laid down by?

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

Answer: D

NEW QUESTION 7
SCENARIO
Please use the following to answer the next question:
Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.
Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.
Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.
In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.
Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.
In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.
Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly
owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.
Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.
After Louis has exercised his right to restrict the use of his data, under what conditions would Accidentable have grounds for refusing to comply?

A. If Accidentable is entitled to use of the data as an affiliate of Bedrock.
B. If Accidentable also uses the data to conduct public health research.
C. If the data becomes necessary to defend Accidentable's legal rights.
D. If the accuracy of the data is not an aspect that Louis is disputing.

Answer: A

NEW QUESTION 8
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 9
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 10
What is the consequence if a processor makes an independent decision regarding the purposes and means of processing it carries out on behalf of a controller?

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

Answer: B

NEW QUESTION 10
Which area of privacy is a lead supervisory authority's (LSA) MAIN concern?

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

Answer: C

NEW QUESTION 12
When does the GDPR provide more latitude for a company to process data beyond its original collection purpose?

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

Answer: C

NEW QUESTION 17
To provide evidence of GDPR compliance, a company performs an internal audit. As a result, it finds a data base, password-protected, listing all the social network followers of the client.
Regarding the domain of the controller-processor relationships, how is this situation considered?

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

Answer: B

NEW QUESTION 19
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 22
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 26
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 27
What type of data lies beyond the scope of the General Data Protection Regulation?

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

Answer: B

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

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

Answer: D

NEW QUESTION 34
A company is hesitating between Binding Corporate Rules and Standard Contractual Clauses as a global data transfer solution. Which of the following statements would help the company make an effective decision?

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

Answer: C

NEW QUESTION 37
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 41
When hiring a data processor, which action would a data controller NOT be able to depend upon to avoid liability in the event of a security breach?

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

Answer: A

NEW QUESTION 44
An employee of company ABCD has just noticed a memory stick containing records of client data, including their names, addresses and full contact details has disappeared. The data on the stick is unencrypted and in clear text. It is uncertain what has happened to the stick at this stage, but it likely was lost during the travel of an employee. What should the company do?

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

Answer: A

NEW QUESTION 45
How does the GDPR now define "processing"?

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

Answer: A

NEW QUESTION 46
SCENARIO
Please use the following to answer the next question:
BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information – name, location, and prior purchase history – with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens.
Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.
What is the nature of BHealthy and Natural Insight's relationship?

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

Answer: A

NEW QUESTION 51
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 52
SCENARIO
Please use the following to answer the next question:
Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA. Today, it is a multi-billion-dollar candy company operating in every continent. All of the company's IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father's company, but is also secretly working on launching a new global online dating website company called Ben Knows Best.
Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company's online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers' philosophical beliefs, political opinions and marital status.
If a customer identifies as single, Ben then copies all of that customer's personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out.
Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.
Joe also hires his best friend's daughter, Alice, who just graduated from law school in the U.S., to be the company's new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company's operations in the European Union to the U.S.
Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company's IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone's information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.
In preparing the company for its impending lawsuit, Alice's instruction to the company's IT Department violated Article 5 of the GDPR because the company failed to first do what?

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

Answer: B

NEW QUESTION 53
SCENARIO
Please use the following to answer the next question:
Sandy recently joined Market4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.
Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.
What is the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U?

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

Answer: A

NEW QUESTION 58
In which scenario is a Controller most likely required to undertake a Data Protection Impact Assessment?

A. When the controller is collecting email addresses from individuals via an online registration form for marketing purposes.
B. When personal data is being collected and combined with other personal data to profile the creditworthiness of individuals.
C. When the controller is required to have a Data Protection Officer.
D. When personal data is being transferred outside of the EEA.

Answer: C

NEW QUESTION 60
Which of the following is NOT considered a fair processing practice in relation to the transparency principle?

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

Answer: A

NEW QUESTION 62
In which of the following cases would an organization MOST LIKELY be required to follow both ePrivacy and data protection rules?

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

Answer: A

NEW QUESTION 65
A U.S.-based online shop uses sophisticated software to track the browsing behavior of its European customers and predict future purchases. It also shares this information with third parties. Under the GDPR, what is the online shop's PRIMARY obligation while engaging in this kind of profiling?

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

Answer: A

NEW QUESTION 68
With respect to international transfers of personal data, the European Data Protection Board (EDPB) confirmed that derogations may be relied upon under what condition?

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

Answer: B

NEW QUESTION 70
When does the European Data Protection Board (EDPB) recommend reevaluating whether a transfer tool is effectively providing a level of personal data protection that is in compliance with the European Union (EU) level?

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

Answer: C

NEW QUESTION 74
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 77
After leaving the EU under the terms of Brexit, the United Kingdom will seek an adequacy determination. What is the reason for this?

A. The Insurance Commissioner determined that an adequacy determination is required by the Data Protection Act.
B. Adequacy determinations automatically lapse when a Member State leaves the EU.
C. The UK is now a third country because it's no longer subject to the GDPR.
D. The UK is less trustworthy now that its not part of the Union.

Answer: C

NEW QUESTION 81
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 84
The European Parliament jointly exercises legislative and budgetary functions with which of the following?

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

Answer: C

NEW QUESTION 85
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
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 90
SCENARIO
Please use the following to answer the next question:
Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.
The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.
In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures. Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.
What must Zandelay provide to the supervisory authority during the prior consultation?

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

Answer: B

NEW QUESTION 91
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 94
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 98
SCENARIO
Please use the following to answer the next question:
Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA. Today, it is a multi-billion-dollar candy company operating in every continent. All of the company's IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father's company, but is also secretly working on launching a new global online dating website company called Ben Knows Best.
Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company's online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers' philosophical beliefs, political opinions and marital status.
If a customer identifies as single, Ben then copies all of that customer's personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out.
Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.
Joe also hires his best friend's daughter, Alice, who just graduated from law school in the U.S., to be the company's new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company's operations in the European Union to the U.S.
Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company's IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone's information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.
As a result of Sam's actions, the Gummy Bear Company potentially violated Articles 33 and 34 of the GDPR and will be required to do what?

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

Answer: A

NEW QUESTION 99
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 101
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 102
Bioface is a company based in the United States. It has no servers, personnel or assets in the European Union. By collecting photographs from social media and other web-based services, such as newspapers and blogs, it uses machine learning to develop a facial recognition algorithm. The algorithm identifies individuals in photographs who are not in its data set based the algorithm and its existing data. The service collects photographs of data subjects in the European Union and will identify them if presented with their photographs. Bioface offers its service to government agencies and companies in the United States and Canada, but not to those in the European Union. Bioface does not offer the service to individuals.
Why is Bioface subject to the territorial scope of the General Data Protection Regulation?

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

Answer: A

NEW QUESTION 104
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 106
SCENARIO
Please use the following to answer the next question:
WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids' website states the following:
"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the data. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information.
We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."
"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."
"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities."
What must the contract between WonderKids and the hosting service provider contain?

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

Answer: A

NEW QUESTION 107
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 111
When may browser settings be relied upon for the lawful application of cookies?

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

Answer: B

NEW QUESTION 115
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 120
Under the GDPR, where personal data is not obtained directly from the data subject, a controller is exempt from directly providing information about processing to the data subject if?

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

Answer: A

NEW QUESTION 124
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 128
Which GDPR principle would a Spanish employer most likely depend upon to annually send the personal data of its employees to the national tax authority?

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

Answer: B

NEW QUESTION 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 136
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 137
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 138
Which of the following is an example of direct marketing that would be subject to European data protection laws?

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

Answer: B

NEW QUESTION 141
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 142
SCENARIO
Please use the following to answer the next question:
Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.
The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.
In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures, Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.
What would MOST effectively assist Zandelay in conducting their data protection impact assessment?

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

Answer: A

NEW QUESTION 144
SCENARIO
Please use the following to answer the next question:
T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.
T-C raze also opened various office locations throughout Europe to help expand its business. While Germany 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 147
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 151
In which situation would a data controller most likely be able to justify the processing of the data of a child without parental consent?

A. When the data is to be processed for market research.
B. When providing preventive or counselling services to the child.
C. When providing the child with materials purely for educational use.
D. When a legitimate business interest makes obtaining consent impractical.

Answer: B

NEW QUESTION 155
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
Pursuant to Article 4(5) of the GDPR, data is considered “pseudonymized” if?

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

Answer: A

NEW QUESTION 164
SCENARIO
Please use the following to answer the next question:
Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers’ data to third parties, and he’s convinced that Accidentable must have gotten his information from Bedrock Insurance.
Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.
Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.
In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.
Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis’s contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.
In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.
Accidentable’s response letter confirms Louis’s suspicions. Accidentable is Bedrock Insurance’s wholly owned subsidiary, and they received information about Louis’s accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis’s contract included, a provision in which he agreed to share his information with Bedrock’s affiliates for business purposes.
Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.
Which statement accurately summarizes Bedrock’s obligation in regard to Louis’s data portability request?

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

Answer: B

NEW QUESTION 165
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 168
Which of the following is NOT a role of works councils?

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

Answer: C

NEW QUESTION 173
What was the aim of the European Data Protection Directive 95/46/EC?

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

Answer: B

NEW QUESTION 174

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

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

Answer: A

NEW QUESTION 178
Which of the following is NOT an explicit right granted to data subjects under the GDPR?

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

Answer: A

NEW QUESTION 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 Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.
Joe also hires his best friend's daughter, Alice, who just graduated from law school in the U.S., to be the company's new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company's operations in the European Union to the U.S.
Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company's IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone's information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.
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 183
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 186
Which marketing-related activity is least likely to be covered by the provisions of Privacy and Electronic Communications Regulations (Directive 2002/58/EC)?

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

Answer: A

NEW QUESTION 187
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 192
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 197
A key component of the OECD Guidelines is the "Individual Participation Principle". What parts of the General Data Protection Regulation (GDPR) provide the closest equivalent to that principle?

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

Answer: D

NEW QUESTION 200
A data controller appoints a data protection officer. Which of the following conditions would NOT result in an infringement of Articles 37 to 39 of the GDPR?

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

Answer: D

NEW QUESTION 205
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 206
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan
to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
With regard to TripBliss Inc.'s use of website cookies, which of the following statements is correct?

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

Answer: B

NEW QUESTION 208
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 213
SCENARIO
Please use the following to answer the next question:
Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:
Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.
Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).
Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees.
These records are available to former students after registering through Granchester's Alumni portal. Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.
Under their security policy, the University encrypts all of its personal data records in transit and at rest.
In order to improve his teaching, Frank wants to investigate how his engineering students perform in relational to Department for Education expectations. He has attended one of Anna's data protection training courses and knows that he should use no more personal data than necessary to accomplish his goal. He creates a program that will only export some student data: previous schools attended, grades originally obtained, grades currently obtained and first time university attended. He wants to keep the records at the individual student level. Mindful of Anna's training, Frank runs the student numbers through an algorithm to transform them into different reference numbers. He uses the same algorithm on each occasion so that he can update each record over time.
One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs
Anna about his performance database.
Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.
Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.
Which of the University's records does Anna NOT have to include in her record of processing activities?

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

Answer: C

NEW QUESTION 218
The GDPR specifies fines that may be levied against data controllers for certain infringements. Which of the following infringements would be subject to the less severe administrative fine of up to 10 million euros (or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year)?

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

Answer: D

NEW QUESTION 221
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 224
SCENARIO
Please use the following to answer the next question:
Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.
The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre- registrations, it will develop EU-specific content and services.
Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
The Customer for Life plan may conflict with which GDPR provision?

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

Answer: B

NEW QUESTION 229
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.
Under the GDPR, Liem and EcoMick's contract with MarketIQ must include all of the following provisions EXCEPT?

A. Processing the personal data upon documented instructions regarding data transfers outside of the EEA.
B. Notification regarding third party requests for access to Liem and EcoMick's personal data.
C. Assistance to Liem and EcoMick in their compliance with data protection impact assessments.
D. Returning or deleting personal data after the end of the provision of the services.

Answer: C

NEW QUESTION 233
SCENARIO
Please use the following to answer the next question:
The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal

department.
Registration Form
Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)
Vigotron values your privacy. The M-Heaith app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)
Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third- party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.
We are happy to offer the M-Health app free of charge. If you want to download and use it, we ask that you first complete this registration form. (Please note that use of the M-Health app is restricted to adults aged 16 or older, unless parental consent has been given to minors intending to use it.)

First name:
Surname:
Year of birth:
Email:
Physical Address (optional*):
Health status:
*If you are interested in receiving newsletters about our products and services that we think may be of interest to you, please include your physical address. If you decide later that you do not wish to receive these newsletters, you can unsubscribe by sending an email to unsubscribe@vigotron.com or send a letter with your request to the address listed at the bottom of this page.
Terms and Conditions 1.Jurisdiction. […] 2.Applicable law. […] 3.Limitation of liability. […] Consent
By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.
Emily sends the draft to Sam for review. Which of the following is Sam most likely to point out as the biggest problem with Emily's consent provision?

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

Answer: C

NEW QUESTION 237
Which of the following demonstrates compliance with the accountability principle found in Article 5, Section 2 of the GDPR?

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

Answer: B

NEW QUESTION 239
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 242
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files

onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
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 243
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 248
In addition to the European Commission, who can adopt standard contractual clauses, assuming that all required conditions are met?

A. Approved data controllers.
B. The Council of the European Union.
C. National data protection authorities.
D. The European Data Protection Supervisor.

Answer: A

NEW QUESTION 250
SCENARIO
Please use the following to answer the next question:
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B.
Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:
Name
Address
Date of Birth
Payroll number
National Insurance number
Sick pay entitlement
Maternity/paternity pay entitlement
Holiday entitlement
Pension and benefits contributions
Trade union contributions
Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B. This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to
Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she notifies all affected employees.
Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?

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

Answer: C

NEW QUESTION 252
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 254
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CIPP-E Practice Exam Features:

* CIPP-E Questions and Answers Updated Frequently

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

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

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