IAPP

Exam Questions CIPP-E

Certified Information Privacy Professional/Europe (CIPP/E)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
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 3
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 4
Which of the following does NOT have to be included in the records most processors must maintain in relation to their data processing activities?

A. Name and contact details of each controller on behalf of which the processor is acting.
B. Categories of processing carried out on behalf of each controller for which the processor is acting.
C. Details of transfers of personal data to a third country carried out on behalf of each controller for which the processor is acting.
D. Details of any data protection impact assessment conducted in relation to any processing activities carried out by the processor on behalf of each controller for which the processor is acting.

Answer: C

NEW QUESTION 5
An online company's privacy practices vary due to the fact that it offers a wide variety of services. How could it best address the concern that explaining them all would make the policies incomprehensible?

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

Answer: B

NEW QUESTION 6
Which statement is correct when considering the right to privacy under Article 8 of the European Convention on Human Rights (ECHR)?

A. The right to privacy is an absolute right
B. The right to privacy has to be balanced against other rights under the ECHR
C. The right to freedom of expression under Article 10 of the ECHR will always override the right to privacy
D. The right to privacy protects the right to hold opinions and to receive and impart ideas without interference

Answer: B

NEW QUESTION 7
Data retention in the EU was underpinned by a legal framework established by the Data Retention Directive (2006/24/EC). Why is the Directive no longer part of EU law?

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

Answer: C

NEW QUESTION 8
To provide evidence of GDPR compliance, a company performs an internal audit. As a result, it finds a data base, password-protected, listing all the social network followers of the client.
Regarding the domain of the controller-processor relationships, how is this situation considered?

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

Answer: B

NEW QUESTION 9
What is one major goal that the OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) all had in common but largely failed to achieve in Europe?

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

Answer: D

NEW QUESTION 10
Which of the following is the weakest lawful basis for processing employee personal data?

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

Answer: B

NEW QUESTION 10
To receive a preliminary interpretation on provisions of the GDPR, a national court will refer its case to which of the following?

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

Answer: A

NEW QUESTION 11
Which aspect of the GDPR will likely have the most impact on the consistent implementation of data protection laws throughout the European Union?

A. That it essentially functions as a one-stop shop mechanism
B. That it takes the form of a Regulation as opposed to a Directive
C. That it makes notification of large-scale data breaches mandatory
D. That it makes appointment of a data protection officer mandatory

Answer: D

NEW QUESTION 12

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 14
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 15
A well-known video production company, based in Spain but specializing in documentaries filmed worldwide, has just finished recording several hours of footage featuring senior citizens in the streets of Madrid. Under what condition would the company NOT be required to obtain the consent of everyone whose image they use for their documentary?

A. If obtaining consent is deemed to involve disproportionate effort.
B. If obtaining consent is deemed voluntary by local legislation.
C. If the company limits the footage to data subjects solely of legal age.
D. If the company's status as a documentary provider allows it to claim legitimate interest.

Answer: B

NEW QUESTION 17
Article 5(1)(b) of the GDPR states that personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Based on Article 5(1)(b),
what is the impact of a member state's interpretation of the word "incompatible"?

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

Answer: A

NEW QUESTION 20
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 23
Under the GDPR, who would be LEAST likely to be allowed to engage in the collection, use, and disclosure of a data subject’s sensitive medical information without the data subject’s knowledge or consent?

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

Answer: B

NEW QUESTION 28
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 29
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 32
Which institution has the power to adopt findings that confirm the adequacy of the data protection level in a non-EU country?

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

Answer: B

NEW QUESTION 37
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 40
What is the MAIN reason GDPR Article 4(22) establishes the concept of the “concerned supervisory authority”?

A. To encourage the consistency of local data processing activity.
B. To give corporations a choice about who their supervisory authority will be.

C. To ensure the GDPR covers controllers that do not have an establishment in the EU but have a representative in a member state.
D. To ensure that the interests of individuals residing outside the lead authority's jurisdiction are represented.

Answer: A

NEW QUESTION 42
SCENARIO
Please use the following to answer the next question:
Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:

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

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

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

One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs Anna about his performance database.
Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.
Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.
Anna will find that a risk analysis is NOT necessary in this situation as long as?

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

Answer: D

NEW QUESTION 46
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.
To ensure GDPR compliance, what should be the company's position on the issue of consent?

A. The child, as the user of the action figure, can provide consent himself, as long as no information is shared for marketing purposes.
B. Written authorization attesting to the responsible use of children's data would need to be obtained from the supervisory authority.
C. Consent for data collection is implied through the parent's purchase of the action figure for the child.
D. Parental consent for a child's use of the action figures would have to be obtained before any data could be collected.

Answer: D

NEW QUESTION 50
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 53
SCENARIO
Please use the following to answer the next question:
ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an
internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.
Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain's locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.
Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.
In which of the following situations would ABC Hotel Chain and XYZ Travel Agency NOT have to honor Mike's data access request?

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

Answer: C

NEW QUESTION 54
A company in France suffers a robbery over the weekend owing to a faulty alarm system. When it is determined that the break-in involves the loss of a substantial amount of data, the company decides on a CCTV system to monitor for future incidents. Company technicians install cameras in the entrance of the building, hallways and offices. Footage is recorded continuously, and is monitored by the home office in the United States. What is the most realistic step the company could take to address their security concerns and comply with the personal data processing principles set out in Article 5 of the GDPR?

A. Seek informed consent from company employees.
B. Have cameras recording during work hours only.
C. Retain captured footage for no more than 30 days.
D. Restrict camera placement to building entrances only.

Answer: A

NEW QUESTION 58
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 62
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 65
Which of the following would require designating a data protection officer?

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

Answer: D

NEW QUESTION 70
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 72
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 76
An organization receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal data. Under what condition can the organization charge the data subject a fee for processing the request?

A. Only where the organization can show that it is reasonable to do so because more than one request was made.
B. Only to the extent this is allowed under the restrictions on data subjects' rights introduced under Art 23 of GDPR.
C. Only where the administrative costs of taking the action requested exceeds a certain threshold.
D. Only if the organization can demonstrate that the request is clearly excessive or misguided.

Answer: B

NEW QUESTION 81
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 85
SCENARIO
Please use the following to answer the next question:
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:

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

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

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

Answer: A

NEW QUESTION 86
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 87
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 88
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 91
A worker in a European Union (EU) member state has ceased his employment with a company. What should the employer most likely do in regard to the worker's personal data?

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

Answer: A

NEW QUESTION 92
Which GDPR requirement will present the most significant challenges for organizations with Bring Your Own Device (BYOD) programs?

A. Data subjects must be sufficiently informed of the purposes for which their personal data is processed.
B. Processing of special categories of personal data on a large scale requires appointing a DPO.
C. Personal data of data subjects must always be accurate and kept up to date.
D. Data controllers must be in control of the data they hold at all times.

Answer: D

NEW QUESTION 96
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 100
The GDPR forbids the practice of "forum shopping", which occurs when companies do what?

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

Answer: B

NEW QUESTION 101
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 102
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 105
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 110
The Planet 49 CJEU Judgement applies to?

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

Answer: C

NEW QUESTION 113
WP29's "Guidelines on Personal data breach notification under Regulation 2016/679'' provides examples of ways to communicate data breaches transparently. Which of the following was listed as a method that would NOT be effective for communicating a breach to data subjects?

A. A postal notification
B. A direct electronic message
C. A notice on a corporate blog
D. A prominent advertisement in print media

Answer: C

NEW QUESTION 115
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 118
Under what circumstances would the GDPR apply to personal data that exists in physical form, such as information contained in notebooks or hard copy files?

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

Answer: D

NEW QUESTION 122
How is the retention of communications traffic data for law enforcement purposes addressed by European data protection law?

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

Answer: D

NEW QUESTION 124
A Spanish electricity customer calls her local supplier with Questions: about the company's upcoming merger. Specifically, the customer wants to know the recipients to whom her personal data will be disclosed once the merger is final. According to Article 13 of the GDPR, what must the company do before providing the customer with the requested information?

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

Answer: A

NEW QUESTION 125
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 130
SCENARIO
Please use the following to answer the next question:
Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.
Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.
After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.
Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.
In addition to notifying employees about the purpose of the monitoring, the potential uses of their data and their privacy rights, what information should Building Block have provided them before implementing the security measures?

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

Answer: A

NEW QUESTION 133
Which sentence BEST summarizes the concepts of "fairness," "lawfulness" and "transparency", as expressly required by Article 5 of the GDPR?

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

Answer: A

NEW QUESTION 136
Which of the following would NOT be relevant when determining if a processing activity would be considered profiling?

A. If the processing is to be performed by a third-party vendor
B. If the processing involves data that is considered personal data
C. If the processing of the data is done through automated means
D. If the processing is used to predict the behavior of data subjects

Answer: D

NEW QUESTION 137
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 138
Which mechanism, new to the GDPR, now allows for the possibility of personal data transfers to third countries under Article 42?

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

Answer: A

NEW QUESTION 142
What is the key difference between the European Council and the Council of the European Union?

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

Answer: D

NEW QUESTION 145
A company is located in a country NOT considered by the European Union (EU) to have an adequate level of data protection. Which of the following is an obligation of the company if it imports personal data from another organization in the European Economic Area (EEA) under standard contractual clauses?

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

Answer: A

NEW QUESTION 150
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 153
Tanya is the Data Protection Officer for Curtains Inc., a GDPR data controller. She has recommended that the company encrypt all personal data at rest. Which GDPR principle is she following?

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

Answer: C

NEW QUESTION 154
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 157
If a company is planning to use closed-circuit television (CCTV) on its premises and is concerned with GDPR compliance, it should first do all of the following EXCEPT?

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

Answer: C

NEW QUESTION 160
.....

Relate Links

100% Pass Your CIPP-E Exam with Exambible Prep Materials

https://www.exambible.com/CIPP-E-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/