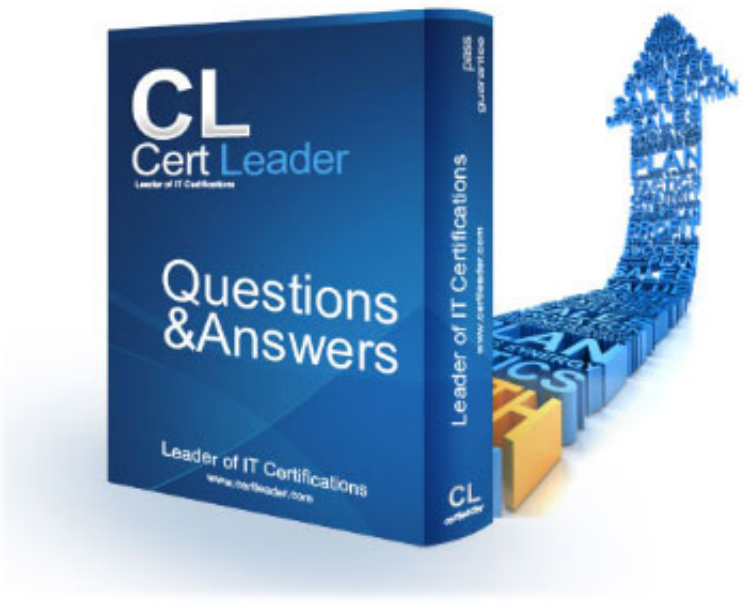
CIPP-E Dumps

Certified Information Privacy Professional/Europe (CIPP/E)

https://www.certleader.com/CIPP-E-dumps.html



NEW QUESTION 1
Article 29 Working Party has emphasized that the GDPR forbids “forum shopping”, which occurs when companies do what?

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

Answer: B

NEW QUESTION 2
With the issue of consent, the GDPR allows member states some choice regarding what?

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

Answer: C

NEW QUESTION 3
A German data subject was the victim of an embarrassing prank 20 years ago. A newspaper website published an article about the prank at the time, and the article is still available on the newspaper’s website. Unfortunately, the prank is the top search result when a user searches on the victim’s name. The data subject requests that SearchCo delist this result. SearchCo agrees, and instructs its technology team to avoid scanning or indexing the article. What else must SearchCo do?

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

Answer: A

NEW QUESTION 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 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 6
Which type of personal data does the GDPR define as a “special category” of personal data?

A. Educational history.
B. Trade-union membership.
C. Closed Circuit Television (CCTV) footage.
D. Financial information.

Answer: B

NEW QUESTION 7
Which change was introduced by the 2009 amendments to the e-Privacy Directive 2002/58/EC?

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

Answer: D

NEW QUESTION 8
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 9
Which of the following is the weakest lawful basis for processing employee personal data?

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

Answer: B

NEW QUESTION 10
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.
If a user of the M-Health app were to decide to withdraw his consent, Vigotron would first be required to do what?

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

Answer: D

NEW QUESTION 10
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 14
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 19
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 24
Article 9 of the GDPR lists exceptions to the general prohibition against processing biometric data. Which of the following is NOT one of these exceptions?

A. The processing is done by a non-profit organization and the results are disclosed outside the organization.
B. The processing is necessary to protect the vital interests of the data subject when he or she is incapable of giving consent.
C. The processing is necessary for the establishment, exercise or defense of legal claims when courts are acting in a judicial capacity.
D. The processing is explicitly consented to by the data subject and he or she is allowed by Union or Member State law to lift the prohibition.

Answer: A

NEW QUESTION 25
Article 58 of the GDPR describes the power of supervisory authorities. Which of the following is NOT among those granted?

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

Answer: D

NEW QUESTION 28
Read the following steps:
Discover which employees are accessing cloud services and from which devices and apps Lock down the data in those apps and devices
Monitor and analyze the apps and devices for compliance
Manage application life cycles
Monitor data sharing
An organization should perform these steps to do which of the following?

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

Answer: C

NEW QUESTION 31
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 34
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 37
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 41
With respect to international transfers of personal data, the European Data Protection Board (EDPB) confirmed that derogations may be relied upon under what condition?

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

Answer: B

NEW QUESTION 45
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 50
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 55
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 60
SCENARIO
Please use the following to answer the next question:
Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.
Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.
After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.
Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.
What would be the MOST APPROPRIATE way for Building Block to handle the situation with the employee from Italy?

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

Answer: D

NEW QUESTION 61
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 64

SCENARIO
Please use the following to answer the next question:
Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.
After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.
Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.
Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.
Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?

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

Answer: B

NEW QUESTION 65
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 68
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 70
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 74
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 79
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 80
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.
What is one potential problem Vigotron’s age policy might encounter under the GDPR?

A. Age restrictions are more stringent when health data is involved.
B. Users are only required to be aged 13 or over to be considered adults.
C. Organizations must make reasonable efforts to verify parental consent.
D. Organizations that tie a service to marketing must seek consent for each purpose.

Answer: A

NEW QUESTION 84
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 86
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 90
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 92
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 93
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 96
An unforeseen power outage results in company Z's lack of access to customer data for six hours. According to article 32 of the GDPR, this is considered a breach. Based on the WP 29's February, 2018 guidance, company Z should do which of the following?

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

Answer: C

NEW QUESTION 101
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 104
When is data sharing agreement MOST likely to be needed?

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

Answer: B

NEW QUESTION 108
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 112
SCENARIO
Please use the following to answer the next question:
ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an
internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.
Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain's locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.
Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.
What is the time period in which Mike should receive a response to his request?

A. Not more than one month of receipt of Mike's request.
B. Not more than two months after verifying Mike's identity.
C. When all the information about Mike has been collected.
D. Not more than thirty days after submission of Mike's request.

Answer: D

NEW QUESTION 113
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 115
An organization conducts body temperature checks as a part of COVID-19 monitoring. Body temperature is measured manually and is not followed by registration, documentation or other processing of an individual's personal data.
Which of the following best explain why this practice would NOT be subject to the GDPR?

A. Body temperature is not considered personal data.
B. The practice does not involve completion by automated means.
C. Body temperature is considered pseudonymous data.
D. The practice is for the purpose of alleviating extreme risks to public health.

Answer: B

NEW QUESTION 118
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CIPP-E Exam with Our Prep Materials Via below:

https://www.certleader.com/CIPP-E-dumps.html