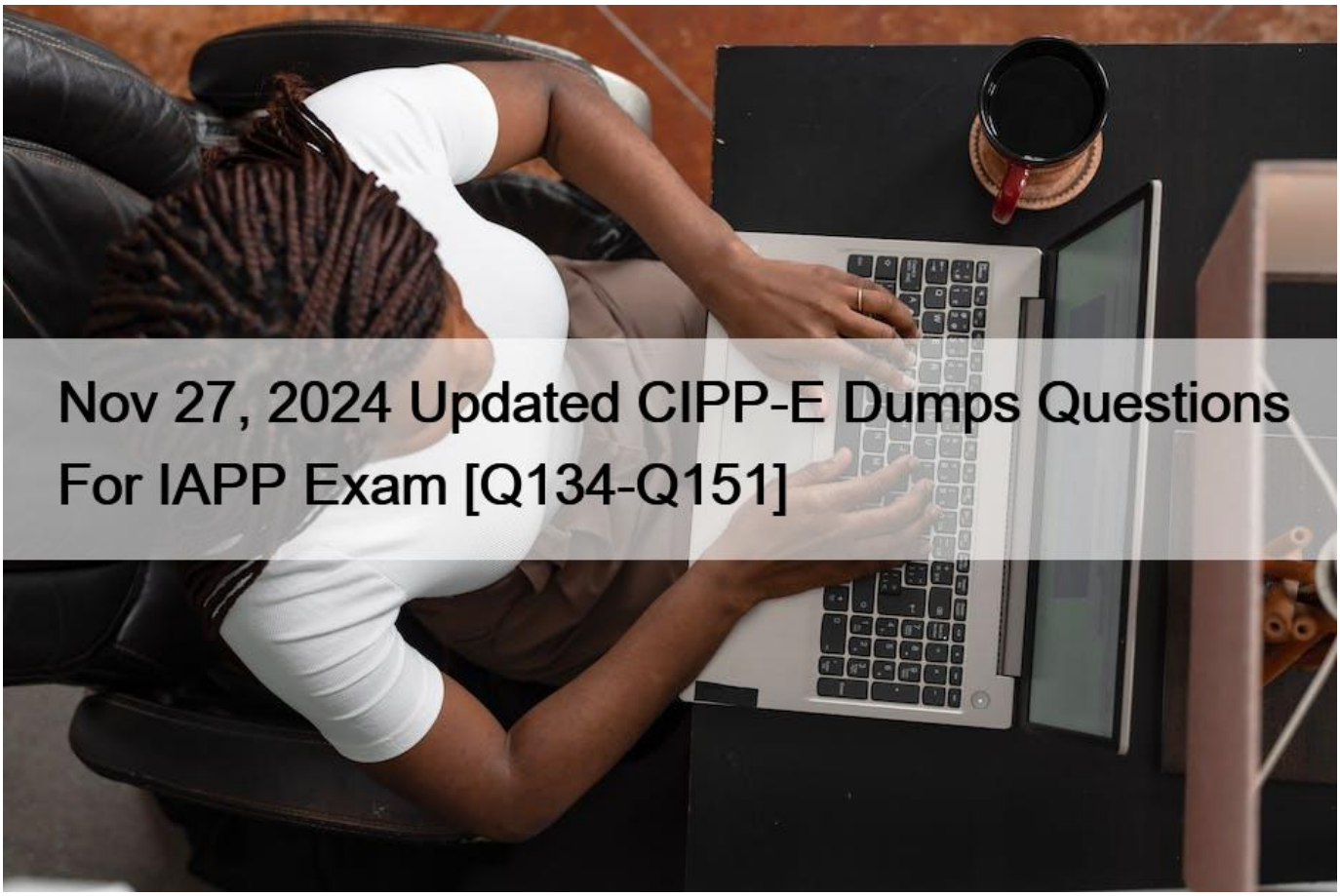
Nov 27, 2024 Updated CIPP-E Dumps Questions For IAPP Exam [Q134-Q151



Nov 27, 2024 Updated CIPP-E Dumps Questions For IAPP Exam
Best Value Available Preparation Guide for CIPP-E Exam

IAPP CIPP-E certification is an essential qualification for professionals who work with personal data and are responsible for ensuring compliance with European data protection laws and regulations. It is a globally recognized certification that demonstrates a professional's competence in data privacy and enhances their credibility in the industry. Certified Information Privacy Professional/Europe (CIPP/E) certification is awarded by the IAPP and is recognized by data protection authorities worldwide.

NO.134 SCENARIO

Please use the following to answer the next question:

Jack worked as a Pharmacovigiliance Operations Specialist in the Irish office of a multinational pharmaceutical company on a clinical trial related to COVID-19. As part of his onboarding process Jack received privacy training He was explicitly informed that while he would need to process confidential patient data in the course of his work, he may under no circumstances use this data for anything other than the performance of work-related (asks This was also specified in the privacy policy, which Jack signed upon

conclusion of the training.

After several months of employment, Jack got into an argument with a patient over the phone. Out of anger he later posted the patient’s name and hearth information, along with disparaging comments, on a social media website. When this was discovered by his Pharmacovigilance supervisors. Jack was immediately dismissed Jack’s lawyer sent a letter to the company stating that dismissal was a disproportionate sanction, and that if Jack was not reinstated within 14 days his firm would have no alternative but to commence legal proceedings against the company. This letter was accompanied by a data access request from Jack requesting a copy of “all personal data, including internal emails that were sent/received by Jack or where Jack is directly or indirectly identifiable from the contents In relation to the emails Jack listed six members of the management team whose inboxes he required access.

The company conducted an initial search of its IT systems, which returned a large amount of information They then contacted Jack, requesting that he be more specific regarding what information he required, so that they could carry out a targeted search Jack responded by stating that he would not narrow the scope of the information requester.

Under Article 82 of the GDPR (“Right to compensation and liability-), which party is liable for the damage caused by the data breach?
* Both parties are exempt, as the company is involved in human health research
* Jack and the pharmaceutical company are jointly liable.
* The pharmaceutical company is liable.
* Jack is liable

NO.135
* 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
* 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?
* Hiring companies whose measures are consistent with recommendations of accrediting bodies.
* Requesting advice and technical support from Company A’s IT team.
* Avoiding the use of another company’s data to improve their own services.
* Vetting companies’ measures with the appropriate supervisory authority.

Explanation/Reference: https://www.knowyourcompliance.com/gdpr-technical-organisational-measures/

NO.136 After detecting an intrusion involving the theft of unencrypted personal data, who shall the breached company notify first under GDPR requirements?
* Any parents of children whose personal data was compromised.
* Any affected customers whose data was compromised.
* A competent supervisory authority.
* A local law enforcement agency

NO.137 What is true if an employee makes an access request to his employer for any personal data held about him?
* The employer can automatically decline the request if it contains personal data about a third person.
* The employer can decline the request if the information is only held electronically.
* The employer must supply all the information held about the employee.
* The employer must supply any information held about an employee unless an exemption applies.

According to the UK GDPR, employees have the right to access and receive a copy of their personal data, and other supplementary information, from their employer. This is known as a data subject access request (DSAR). Employers must respond to a DSAR without delay and within one month of receipt of the request, unless the request is complex or excessive. Employers should perform a reasonable search for the requested information and provide it in an accessible, concise and intelligible format. Employers can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive. Some of the exemptions that may apply in the employment context are: legal privilege, management forecasting, confidential references, negotiations, regulatory functions, and criminal convictions and offences. Employers should disclose the information securely and inform the employee of their rights and the source of the data. Reference:

Right of access | ICO

Subject access request Q and As for employers | ICO

Data Subject Access Request (Employers’ Guide) | DavidsonMorris

NO.138 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 dat a. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron’s cloud provider, Stratculous. (Read more about Stratculous here.) Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer’s name, email address or any

other information gathered from the app to any third- party without a customer’s consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer’s legal rights or protect its business or property.

We are happy to offer the M-Health app free of charge. If you want to download and use it, we ask that you first complete this registration form. (Please note that use of the M-Health app is restricted to adults aged 16 or older, unless parental consent has been given to minors intending to use it.) First name:

Surname:

Year of birth:

Email:

Physical Address (optional*):

Health status:

*If you are interested in receiving newsletters about our products and services that we think may be of interest to you, please include your physical address. If you decide later that you do not wish to receive these newsletters, you can unsubscribe by sending an email to unsubscribe@vigotron.com or send a letter with your request to the address listed at the bottom of this page.

Terms and Conditions

1. Jurisdiction. […]

2. Applicable law. […]

3. Limitation of liability. […]

Consent

By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.

Emily sends the draft to Sam for review. Which of the following is Sam most likely to point out as the biggest problem with Emily’s consent provision?
* It is not legal to include fields requiring information regarding health status without consent.
* Processing health data requires explicit consent, but the form does not ask for explicit consent.
* Direct marketing requires explicit consent, whereas the registration form only provides for a right to object
* The provision of the fitness app should be made conditional on the consent to the data processing for direct marketing.

NO.139 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?
* Not more than one month of receipt of Mike’s request.
* Not more than two months after verifying Mike’s identity.
* When all the information about Mike has been collected.
* Not more than thirty days after submission of Mike’s request.

According to the GDPR, the right of access by the data subject is one of the rights granted to individuals to obtain information about the processing of their personal data by a data controller1. The data controller must provide a copy of the personal data undergoing processing and additional information, such as the purposes, the categories, the recipients, the retention period, the rights, the source, and the automated decision-making of the processing1. The data controller must also inform the data subject of the existence of the right to access and the means to exercise it2.

The GDPR also specifies the time limit for responding to a data subject access request. The data controller must provide the information without undue delay and in any event within one month of receipt of the request1. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests, but the data controller must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay1. The data controller must also verify the identity of the data subject before providing the information, but this verification should not extend the time limit for responding to the request3.

In this scenario, Mike is an EU resident who has booked travel itineraries through XYZ Travel Agency and stayed at ABC Hotel Chain’s locations. Both companies are U.S.-based multinational companies that use a common platform for collecting and sharing their customer data. Mike has signed the agreement to be a rewards program member of XYZ Travel Agency. Mike wants to know what personal information the company holds about him and sends an email requesting access to his data.

Assuming that both companies are subject to the GDPR, either because they offer goods or services to individuals in the EU or because they monitor the behavior of individuals in the EU4, they must comply with the right of access by the data subject and provide Mike with the information he requests. The time period in which Mike should receive a response to his request is not more than one month of receipt of his request, unless there are grounds for extending the period by two further months. The companies must also verify Mike’s identity before providing the information, but this verification should not affect the time limit for responding to the request.

Therefore, the correct answer is A. Not more than one month of receipt of Mike’s request.

NO.140 Which GDPR requirement will present the most significant challenges for organizations with Bring Your Own Device (BYOD) programs?
* Data subjects must be sufficiently informed of the purposes for which their personal data is processed.
* Processing of special categories of personal data on a large scale requires appointing a DPO.
* Personal data of data subjects must always be accurate and kept up to date.
* Data controllers must be in control of the data they hold at all times.

Reference https://blog.rsisecurity.com/why-byod-is-bad-for-gdpr-compliance/

NO.141 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?
* Pursue a GDPR-compliant Privacy by Design process.
* Institute a GDPR-compliant employee monitoring process.
* Maintain a secure Bring Your Own Device (BYOD) program.
* Ensure cloud vendors are complying with internal data use policies.
Explanation/Reference: https://www.itproportal.com/features/heading-off-the-spectre-of-gdpr-compliance-with-secure-byod/

NO.142 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?
* Documenting due diligence steps taken in the pre-contractual stage.
* Conducting a risk assessment to analyze possible outsourcing threats.
* Requiring that the processor directly notify the appropriate supervisory authority.
* Maintaining evidence that the processor was the best possible market choice available.
The GDPR imposes several obligations on data controllers when they engage data processors to process personal data on their behalf. One of these obligations is to ensure that the contract or other legal act between the controller and the processor stipulates that the processor must assist the controller in complying with its obligations under the GDPR, including the obligation to notify personal data breaches to the competent supervisory authority and, where applicable, to the affected data subjects1. However, this does not mean that the processor can directly notify the supervisory authority without the involvement of the controller. The GDPR clearly states that it is the controller’s responsibility to notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the breach2. The processor must only notify the controller without undue delay after becoming aware of the breach3. Therefore, requiring that the processor directly notify the appropriate supervisory authority is not an action that a data controller can depend upon to avoid liability in the event of a security breach, as it would be contrary to the GDPR and the controller’s own obligation. Options A, B and D are actions that a data controller can take to reduce the risk of liability, as they demonstrate that the controller has exercised due diligence, assessed the potential impact of outsourcing, and chosen a reliable and compliant processor. Reference: 1: Article 28(3)(f) of the GDPR 2: Article 33(1) of the GDPR 3: Article 33(2) of the GDPR

NO.143 SCENARIO

Please use the following to answer the next question:

ProStorage is a multinational cloud storage provider headquartered in the Netherlands. Its CEO. Ruth Brown, has developed a two-pronged strategy for growth: 1) expand ProStorage s global customer base and 2) increase ProStorage’s sales force by efficiently onboarding effective teams. Enacting this strategy has recently been complicated by Ruth’s health condition, which has limited her working hours, as well as her ability to travel to meet potential customers. ProStorage’s Human Resources department and Ruth’s Chief of Staff now work together to manage her schedule and ensure that she is able to make all her medical appointments The latter has become especially crucial after Ruth’s last trip to India, where she suffered a medical emergency and was hospitalized m New Delhi Unable to reach Ruths family, the hospital reached out to ProStorage and was able to connect with her Chief of Staff, who in coordination with Mary, the head of HR. provided information to the doctors

based on accommodate on requests Ruth made when she started a: ProStorage In support of Ruth’s strategic goals of hiring more sales representatives, the Human Resources team is focused on improving its processes to ensure that new employees are sourced, interviewed, hired, and onboarded efficiently. To help with this, Mary identified two vendors, HRYourWay, a German based company, and InstaHR, an Australian based company. She decided to have both vendors go through ProStorage’s vendor risk review process so she can work with Ruth to make the final decision. As part of the review process, Jackie, who is responsible for maintaining ProStorage’s privacy program (including maintaining controller BCRs and conducting vendor risk assessments), reviewed both vendors but completed a transfer impact assessment only for InstaHR. After her review of both boasted a more established privacy program and provided third-party attestations, whereas HRYourWay was a small vendor with minimal data protection operations.

Thus, she recommended InstaHR.

ProStorage’s marketing team also worked to meet the strategic goals of the company by focusing on industries where it needed to grow its market share. To help with this, the team selected as a partner UpFinance, a US based company with deep connections to financial industry customers. During ProStorage’s diligence process, Jackie from the privacy team noted in the transfer impact assessment that UpFinance implements several data protection measures including end-to-end encryption, with encryption keys held by the customer.

Notably, UpFinance has not received any government requests in its 7 years of business. Still, Jackie recommended that the contract require UpFinance to notify ProStorage if it receives a government request for personal data UpFinance processes on its behalf prior to disclosing such data.

Why is the additional measure recommended by Jackie sufficient foe using UpFinance?
* UpFinance is an established 7-year-old business.
* UpFinance is in a highly regulated financial industry
* UpFinance is based in a country without surveillance laws.
* UpFinance implements sufficient data protection measures

According to Article 46 of the GDPR, in the absence of an adequacy decision by the European Commission, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. One of the possible appropriate safeguards is the use of standard data protection clauses adopted by the Commission or by a supervisory authority. However, Article 46(5) states that the possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority shall not affect the possibility for the controller or processor to rely upon other appropriate safeguards provided for in paragraph 2 of this Article, provided that they ensure that data subjects have enforceable and effective rights as regards the processing of their data. Therefore, in this case, Jackie’s recommendation of requiring UpFinance to notify ProStorage if it receives a government request for personal data UpFinance processes on its behalf prior to disclosing such data is an additional measure that could be considered as an appropriate safeguard, especially since UpFinance implements several data protection measures, including end-to-end encryption, with encryption keys held by the customer, which would ensure a high level of security and confidentiality of the personal data transferred. Reference:

Article 46 of the GDPR

IAPP CIPP/E Study Guide, page 67

NO.144 SCENARIO

Please use the following to answer the next question:

BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe.

To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information – name, location, and prior purchase history – with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens.

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

In which case would Natural Insight’s use of BHealthy’s data for improvement of its algorithms be considered data processor activity?
* If Natural Insight uses BHealthy’s data for improving price point predictions only for BHealthy.
* If Natural Insight receives express contractual instructions from BHealthy to use its data for improving its algorithms.
* If Natural Insight agrees to be fully liable for its use of BHealthy’s customer information in its product improvement activities.
* If Natural Insight satisfies the transparency requirement by notifying BHealthy’s customers of its plans to use their information for its product improvement activities.
According to the General Data Protection Regulation (GDPR), a data processor is a natural or legal person, agency, public authority, or any other body who processes personal data on behalf of a data controller. A data controller is a natural or legal person, agency, public authority, or any other body who, alone or jointly with others, determines the purposes and means of the processing of personal data. The GDPR imposes specific obligations and responsibilities on both data controllers and data processors, and requires them to enter into a written contract or other legal act that sets out the subject matter, duration, nature, and purpose of the processing, as well as the obligations and rights of the data controller.

In this scenario, BHealthy is the data controller, as it determines the purpose and means of collecting and sharing its customer information with Natural Insight. Natural Insight is the data processor, as it processes the customer information on behalf of BHealthy for the purpose of determining the price point for BHealthy’s new sunscreens. However, Natural Insight also intends to use the customer information for its own purpose of improving its algorithms, which may not be aligned with BHealthy’s purpose or instructions. This may constitute a breach of the data processing contract and the GDPR, as the data processor must only process the personal data on documented instructions from the data controller, unless required to do so by EU or member state law (Article 28(3)(a) of the GDPR).

Therefore, the only case in which Natural Insight’s use of BHealthy’s data for improvement of its algorithms would be considered data processor activity is if Natural Insight receives express contractual instructions from BHealthy to use its data for improving its algorithms. This would mean that BHealthy has given its consent and authorization for Natural Insight to process the data for that specific purpose, and that Natural Insight is acting in accordance with BHealthy’s instructions. In this case, Natural Insight would still be bound by the data processing contract and the GDPR, and would have to comply with the other obligations and requirements of a data processor, such as ensuring the security of the data, respecting the conditions for engaging another processor, assisting the data controller in ensuring compliance with the GDPR, and deleting or returning the data to the data controller after the end of the service.

The other options are not valid cases for data processor activity, as they do not involve the data controller’s instructions or consent. If Natural Insight uses BHealthy’s data for improving price point predictions only for BHealthy, it may still be processing the data for a different purpose than the one for which it was collected and shared, and without BHealthy’s knowledge or approval. If Natural Insight agrees to be fully liable for its use of BHealthy’s customer information in its product improvement activities, it may still be violating the data processing contract and the GDPR, as it is not acting on behalf of the data controller, but for its own benefit. If Natural Insight satisfies the transparency requirement by notifying BHealthy’s customers of its plans to use their information for its product improvement activities, it may still be infringing the data

controller’s rights and obligations, as it is not the data controller’s role to inform the data subjects of the processing activities, and it may not have a lawful basis for processing the data for its own purpose.

Reference:

GDPR

Data Controllers and Processors – GDPR EU

Who does the UK GDPR apply to? | ICO

What Activities Count as Processing Under the GDPR?

What constitutes data processing? – European Commission

NO.145 What is an important difference between the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) in relation to their roles and functions?
* ECHR can rule on issues concerning privacy as a fundamental right, while the CJEU cannot.
* CJEU can force national governments to implement and honor EU law, while the ECHR cannot.
* CJEU can hear appeals on human rights decisions made by national courts, while the ECHR cannot.
* ECHR can enforce human rights laws against governments that fail to implement them, while the CJEU cannot.

NO.146 What are the obligations of a processor that engages a sub-processor?
* The processor must give the controller prior written notice and perform a preliminary audit of the sub- processor.
* The processor must obtain the controller’s specific written authorization and provide annual reports on the sub-processor’s performance.
* The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.
* The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.
Reference https://inplp.com/latest-news/article/gdpr-rights-and-obligations-of-sub-processors/

NO.147 The Planet 49 CJEU Judgement applies to?
* Cookies used only by third parties.
* Cookies that are deemed technically necessary.
* Cookies regardless of whether the data accessed is personal or not.
* Cookies where the data accessed is considered as personal data only.
Reference:

The Planet 49 CJEU Judgement applies to cookies regardless of whether the data accessed is personal or not. The Court of Justice of the European Union (the ‘CJEU’) delivered this judgement on 1 October 2019, in response to a request for a preliminary ruling from the German Federal Court of Justice (the ‘Bundesgerichtshof’) . The case concerned the validity of consent for the use of cookies and similar technologies under the e-Privacy Directive and the GDPR.

The CJEU ruled that Article 5 (3) of the e-Privacy Directive, which requires consent for the storage of, or access to, information stored in the user’s terminal equipment, applies to any information installed or accessed from an individual’s device, regardless of whether it constitutes personal data or not. The Court reasoned that the aim of the provision is to protect the user from interference with his or her private sphere, which may occur irrespective of the nature of the information stored or accessed. Therefore, the consent requirement applies to all cookies and similar technologies, except for those that are strictly necessary for the provision of a service explicitly requested by the user.

The CJEU also clarified that the consent required for cookies under the e-Privacy Directive must comply with the standard of consent under the GDPR, which means that it must be freely given, specific, informed and unambiguous, and given by a clear affirmative action. The Court held that a pre-ticked checkbox does not constitute valid consent, as it does not imply active behaviour by the user. The Court also stated that the user must be provided with clear and comprehensive information about the cookies, including their duration and whether third parties will have access to them. Reference:

Planet 49 Judgment – takeaways for Cookie Monsters

The Planet 49 decision: Implications for organisations that use cookies CURIA – List of results

NO.148 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?
* Assessed potential privacy risks by conducting a data protection impact assessment.
* Consulted with the relevant data protection authority about potential privacy violations.
* Distributed a more comprehensive notice to employees and received their express consent.
* Consulted with the Information Security team to weigh security measures against possible server impacts.

NO.149 In which case would a controller who has undertaken a DPIA most likely need to consult with a supervisory authority?
* Where the DPIA identifies that personal data needs to be transferred to other countries outside of the EEA.
* Where the DPIA identifies high risks to individuals’ rights and freedoms that the controller can take steps to reduce.
* Where the DPIA identifies that the processing being proposed collects the sensitive data of EU citizens.

* Where the DPIA identifies risks that will require insurance for protecting its business interests.

NO.150 A homeowner has installed a motion-detecting surveillance system that films his front doc and entryway. The camera does not film any public areas only areas that are the property of the homeowner. The system has seen declared to the authorities per the homeowner’s country law, and a placard indicating the area is being video monitored is visible when entering the property Why can the homeowner NOT depend on the household exemption with regards to the processing of the video images recorded by the surveillance camera system?
* The surveillance camera system can potentially capture biometric information of the homeowner’s family, which would be considered a processing of special categories of personal data.
* The homeowner has not specified which security measures ore in place as part of the surveillance camera system
* The GDPR specifically excludes surveillance camera images from the household exemption
* The surveillance camera system can potentially film individuals who enter its filming perimeter

NO.151 Which of the following is an accurate statement regarding the “one-stop-shop” mechanism of the GDPR?
* It can result in several lead supervisory authorities in the EU assuming competence over the same data processing activities of an organization.
* It applies only to direct enforcement of data protection supervisory authorities (e.g.. finding a breach), but not to initiating or engaging m court proceedings
* It gives competence to the lead supervisory authority to address privacy issues derived from processes carried out by public authorities established in different countries.
* It allows supervisory authorities concerned (other than the lead supervisory authority) to act against organizations m exceptional cases even if they do not have any type of establishment in the Member State of the respective authority.
The “one-stop-shop” mechanism of the GDPR is a system of co-operation and consistency procedures that aims to ensure that the data protection regulation is enforced uniformly across all member states and calls on the data protection authorities (DPAs) across member states to co-operate with each other and the Commission to ensure consistent application of the GDPR1. The “one-stop-shop” mechanism applies to organisations that conduct cross-border data processing, which means that they process personal data in the context of the activities of their establishments in more than one member state, or that they target or monitor data subjects in more than one member state1. Under the “one-stop-shop” mechanism, such organisations will have to deal primarily with the DPA of the member state where they have their main establishment or their single establishment in the EU, which will act as their lead supervisory authority for all matters related to their cross-border data processing1. The lead supervisory authority will co-ordinate with other concerned supervisory authorities, which are the DPAs of the member states where the data subjects are affected by the data processing1. The lead supervisory authority will have the competence to adopt binding decisions regarding measures to ensure compliance with the GDPR, such as imposing administrative fines or ordering the suspension of data flows1. However, the “one-stop-shop” mechanism does not prevent the concerned supervisory authorities from acting against organisations in exceptional cases, even if they do not have any type of establishment in the member state of the respective authority1. These exceptional cases include the following situations2:

When a complaint is lodged with a supervisory authority, the subject matter relates only to an establishment in its member state or substantially affects data subjects only in its member state; When a supervisory authority is addressing a possible infringement related to the offering of goods or services to data subjects in its member state or to the monitoring of their behaviour in its member state; When a supervisory authority adopts provisional measures intended to produce legal effects in its own member state; When an urgent need to act arises in order to protect the rights and freedoms of data subjects. In these cases, the concerned supervisory authority will inform the lead supervisory authority and the other concerned supervisory authorities, and will try to reach a consensus on the action to be taken2. If no consensus is reached, the consistency mechanism will apply, which involves the intervention of the European Data Protection Board (EDPB) to issue a binding decision on the matter2. Therefore, option D is the correct answer. Reference: Art. 60 GDPR – Cooperation between the lead supervisory authority and the other supervisory authorities concerned, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

Full CIPP-E Practice Test and 270 Unique Questions, Get it Now!:
https://www.examslabs.com/IAPP/Certified-Information-Privacy-Professional/best-CIPP-E-exam-dumps.html]