[Q139-Q163 CIPP-E Certification Exam Dumps Questions in here [Sep-2024

CIPP-E Certification Exam Dumps Questions in here [Sep-2024]
Updated CIPP-E Exam Practice Test Questions

The CIPP-E certification is particularly relevant for professionals who work with personal data and are responsible for ensuring compliance with the General Data Protection Regulation (GDPR). GDPR is a regulation that came into effect in May 2018 and is applicable to all organizations that process personal data of EU citizens, regardless of where the organization is located. The regulation has a significant impact on how personal data is collected, processed, stored, and secured, and failure to comply with GDPR can result in severe penalties.

What is IAPP CIPP/E Exam

IAPP has introduced Certified Information Privacy Professionals (CIPP) certificate for privacy professionals. The CIPP is the global standard for privacy professionals who manage, handle, and access data. Security professionals get a deep insight into security considerations in the European context through the European edition of CIPP which is CIPP/E.
CIPP/E is a unique designation, the only one of its kind, according to its creator the International Association of Privacy Professionals (IAPP). As a response to increasing demand for secure data privacy protection in 2014 IAPP was introduced. In all stages and throughout lifecycles these security protocols are a must. Thus the need for authoritative and certified practitioners is growing. The professionals/ candidates feel highly confident after bagging global certifications as they are able to validate there

skills and abilities.
CIPP/E Exam is a certification exam that is conducted by IAPP to validates candidate knowledge and identifies technology experts that know how to build data privacy architecture from its foundation in the IT industry.
The Certified Information Privacy Professional (CIPP) helps organizations around the world support compliance and risk mitigation practices, and arms practitioners with the insight needed to add more value to their businesses.
After passing this exam, candidates get a certificate from IAPP that helps them to demonstrate their proficiency in data privacy to their clients and employers.

Q139. SCENARIO

Please use the following to answer the next question:

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

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

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

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

In light of the requirements of Article 32 of the GDPR (related to the Security of Processing), which practice should the company institute?
* Encrypt the data in transit over the wireless Bluetooth connection.
* Include dual-factor authentication before each use by a child in order to ensure a minimum amount of security.
* Include three-factor authentication before each use by a child in order to ensure the best level of security possible.
* Insert contractual clauses into the contract between the toy manufacturer and the cloud service provider, since South Africa is outside the European Union.
According to Article 32 of the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing personal data, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and

severity for the rights and freedoms of natural persons. The GDPR also provides some examples of such measures, including the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In this scenario, the company is processing personal data of children, such as their voice, questions, preferences, and location, through the connected toys that use a wireless Bluetooth connection to communicate with smartphones, tablets, cloud servers, and other toys. This poses a high risk to the security of the data, as Bluetooth is a short-range wireless technology that can be easily intercepted, hacked, or compromised by malicious actors. Therefore, the company should encrypt the data in transit over the Bluetooth connection, to prevent unauthorized access, disclosure, or alteration of the data. Encryption is a process of transforming data into an unreadable form, using a secret key or algorithm, that can only be reversed by authorized parties who have the corresponding key or algorithm. Encryption can protect the data from being accessed or modified by anyone who does not have the key or algorithm, thus ensuring the confidentiality and integrity of the data.

The other options are incorrect because:

B) Including dual-factor authentication before each use by a child in order to ensure a minimum amount of security is not a sufficient measure to protect the data in transit over the Bluetooth connection. Dual-factor authentication is a process of verifying the identity of a user by requiring two pieces of evidence, such as a password and a code sent to a phone or email. While this may enhance the security of the user’s account or device, it does not protect the data that is transmitted over the wireless connection, which can still be intercepted, hacked, or compromised by malicious actors. Moreover, dual-factor authentication may not be suitable or convenient for children, who may not have access to a phone or email, or who may forget their passwords or codes.

C) Including three-factor authentication before each use by a child in order to ensure the best level of security possible is not a necessary or proportionate measure to protect the data in transit over the Bluetooth connection. Three-factor authentication is a process of verifying the identity of a user by requiring three pieces of evidence, such as a password, a code sent to a phone or email, and a biometric feature, such as a fingerprint or a face scan. While this may provide a high level of security for the user’s account or device, it does not protect the data that is transmitted over the wireless connection, which can still be intercepted, hacked, or compromised by malicious actors. Furthermore, three-factor authentication may not be appropriate or feasible for children, who may not have access to a phone or email, or who may not have reliable biometric features, or who may find the process too complex or cumbersome.

D) Inserting contractual clauses into the contract between the toy manufacturer and the cloud service provider, since South Africa is outside the European Union, is not a relevant measure to protect the data in transit over the Bluetooth connection. Contractual clauses are legal agreements that specify the obligations and responsibilities of the parties involved in a data transfer, such as the level of data protection, the rights of data subjects, and the remedies for breaches. While contractual clauses may be necessary to ensure the compliance of the data transfer to South Africa, which is a non-EU country that does not have an adequacy decision from the European Commission, they do not address the security of the data that is transmitted over the wireless connection, which can still be intercepted, hacked, or compromised by malicious actors. Moreover, contractual clauses are not a technical or organisational measure, but a legal measure, that falls under a different provision of the GDPR, namely Article 46.

Q140. SCENARIO

Please use the following to answer the next question:

WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the

childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids’ website states the following:

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

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

“We are processing you and your child’s personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child’s personal information; rectify or erase you or your child’s personal information; the right to correction or erasure of you and/or your child’s personal information; object to any processing of you and your child’s personal information. You also have the right to complain to the supervisory authority about our data processing activities.” What additional information must Wonderkids provide in their Privacy Statement?
* How often promotional emails will be sent.
* Contact information of the hosting company.
* Technical and organizational measures to protect data.
* The categories of recipients with whom data will be shared.

According to Article 13 of the GDPR, when personal data are collected from the data subject, the data controller must provide the data subject with the following information, among others1:

The identity and the contact details of the controller and, where applicable, of the controller’s representative; The contact details of the data protection officer, where applicable; The purposes of the processing for which the personal data are intended as well as the legal basis for the processing; The recipients or categories of recipients of the personal data, if any; Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In the scenario, Wonderkids provides some of this information in their Privacy Statement, but not all. They do not specify the categories of recipients with whom they will share the personal data of their customers and their children. They only state that they will share the data with businesses that they see as adding real value to the customers, which is vague and ambiguous. This does not comply with the GDPR requirement to inform the data subjects about the recipients or categories of recipients of their personal data, if any. Therefore, Wonderkids must provide this additional information in their Privacy Statement.

Reference:

1: Art. 13 GDPR Information to be provided where personal data are collected from the data subject

Q141. 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 medical organization that wants to begin genetic testing to support earlier research for which they have performed a DPIA.
* A data controller who plans to use a new technology product that has already undergone a DPIA by the product’s

provider.
* A marketing team that wants to collect mailing addresses of customers for whom they already have email addresses.
* A railway operator who plans to evaluate the same video surveillance in all the train stations of his company.

Q142. SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

Who-R-U is NOT required to notify the local German DPA about the laptop theft because?
* The company isn’t a controller established in the Union.
* The laptop belonged to a company located in Canada.
* The data isn’t considered personally identifiable financial information.
* There is no evidence that the thieves have accessed the data on the laptop.

Q143. Article 9 of the GDPR lists exceptions to the general prohibition against processing biometric dat a. Which of the following is NOT one of these exceptions?
* The processing is done by a non-profit organization and the results are disclosed outside the organization.
* The processing is necessary to protect the vital interests of the data subject when he or she is incapable of giving consent.
* The processing is necessary for the establishment, exercise or defense of legal claims when courts are acting in a judicial capacity.
* 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.
Article 9 of the GDPR prohibits the processing of special category data, which includes biometric data for the purpose of uniquely identifying a natural person1. However, there are 10 exceptions to this general prohibition, usually referred to as ‘conditions for processing special category data’2. These are:

(a) Explicit consent

(b) Employment, social security and social protection (if authorised by law)

Vital interests

(d) Not-for-profit bodies

(e) Made public by the data subject

(f) Legal claims and judicial acts

(g) Substantial public interest conditions

(h) Health or social care

(i) Public health

(j) Archiving, research and statistics

Option A is not one of these exceptions, and therefore it is not a valid reason to process biometric data under Article 9. Option B, C and D are all valid exceptions, as they correspond to conditions , (f) and (a) respectively. Therefore, the correct answer is A.

Reference:

4: Art. 9 GDPR Processing of special categories of personal data

6: What are the rules on special category data? | ICO

Q144. Which kind of privacy notice, originally advocated by the Article 29 Working Party, is commonly recommended tor Al-based technologies because of the way it provides processing information at specific points of data collection?
* Privacy dashboard notice
* Visualization notice.
* Just-in-lime notice.
* Layered notice.

According to the Article 29 Working Party, a just-in-time notice is a type of privacy notice that provides processing information at specific points of data collection, such as when the user clicks on a certain feature or enters personal data1. This kind of notice is commonly recommended for AI-based technologies because it allows the user to receive relevant and timely information about the processing of their data, without being overwhelmed by lengthy and complex privacy statements1. A just-in-time notice can also be combined with other types of notices, such as layered notices or privacy dashboards, to provide a more comprehensive and user-friendly transparency framework1. Therefore, option C is the correct answer. Option A is incorrect because a privacy dashboard notice is a type of notice that provides the user with a centralised and interactive overview of the processing of their data, and allows them to manage their privacy settings and preferences1. Option B is incorrect because a visualization notice is a type of notice that uses graphical elements, such as icons, symbols, colours, or animations, to convey the processing information in a more intuitive and engaging way1. Option D is incorrect because a layered notice is a type of notice that provides the processing information in a

hierarchical and modular way, starting with the most essential information and allowing the user to access more details if they wish1. Reference:

What’s new in WP29’s final guidelines on transparency?

Q145. Which of the following would MOST likely trigger the extraterritorial effect of the GDPR, as specified by Article

3?
* The behavior of suspected terrorists being monitored by EU law enforcement bodies.
* Personal data of EU citizens being processed by a controller or processor based outside the EU.
* The behavior of EU citizens outside the EU being monitored by non-EU law enforcement bodies.
* Personal data of EU residents being processed by a non-EU business that targets EU customers.

Explanation/Reference: https://hsfnotes.com/data/2019/12/02/edpb-adopts-final-guidelines-on-gdpr-extra-territoriality/

Q146. According to the European Data Protection Board, data subjects should be aware of any video surveillance in operation. How should a retail shop operator ensure that data subjects receive at information required for such a purpose under EU data protection law?
* The shop operator should post a copy of the manual of the video surveillance system in the shop and on its social media channels.
* The shop operator should provide full notice of the intended video surveillance outside the shop, for example with a sign or a stand-up display.
* The shop operator should instruct the data protection officer to hand out a comprehensive notice to data subjects every time they enter the shop.
* The shop operator should provide the most important information on a clearly readable warning sign to data subjects before they enter the monitored area, and additional mandatory details by other means.

Q147. Many businesses print their employees’ photographs on building passes, so that employees can be identified by security staff. This is notwithstanding the fact that facial images potentially qualify as biometric data under the GDPR. Why would such practice be permitted?
* Because use of biometric data to confirm the unique identification of data subjects benefits from an exemption.
* Because photographs qualify as biometric data only when they undergo a “specific technical processing”.
* Because employees are deemed to have given their explicit consent when they agree to be photographed by their employer.
* Because photographic ID is a physical security measure which is “necessary for reasons of substantial public interest”.

According to Recital 51 of the GDPR, photographs are not automatically considered as biometric data, unless they are processed by a specific technical means that allows the unique identification or authentication of a natural person1. This means that printing employees’ photographs on building passes does not necessarily involve biometric data, as long as the photographs are not used for facial recognition or other similar purposes. The other options are incorrect, as they do not reflect the definition of biometric data or the conditions for processing special categories of personal data under the GDPR2. Reference:

Recital 51 of the GDPR

ICO guidance on special category data

Reference https://ess.csa.canon.com/rs/206-CLL-191/images/IAPP-Top-10-Operational-Impacts-of-GDPR.pdf?TC=DM&CN=CSA_OMNIA_Partners&CS=CSA&CR=T1_Gov%20GenNonProfit (11)

Q148. 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.

Q149. A company is located in a country NOT considered by the European Union (EU) to have an adequate level of data protection. Which of the following is an obligation of the company if it imports personal data from another organization in the European Economic Area (EEA) under standard contractual clauses?
* Submit the contract to its own government authority.
* Ensure that notice is given to and consent is obtained from data subjects.
* Supply any information requested by a data protection authority (DPA) within 30 days.
* Ensure that local laws do not impede the company from meeting its contractual obligations.

The GDPR allows the transfer of personal data to countries outside of the EEA that do not provide an adequate level of data protection, if appropriate safeguards are provided by the data exporter and the data importer1. One of these safeguards are standard contractual clauses (SCCs) adopted by the European Commission, which are model clauses that impose obligations on both parties to ensure that the transfer complies with the GDPR requirements2. The SCCs also include clauses on the rights of the data subjects, the obligations of the data protection authorities, and the liability and indemnification of the parties3. One of the obligations of the data importer under the SCCs is to warrant that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract, and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the SCCs, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract4. Therefore, option D is the correct answer, as it reflects the obligation of the data importer under the SCCs to ensure that local laws do not impede the company from meeting its contractual obligations. Options A, B and C are incorrect, as they are not obligations of the data importer under the SCCs. Option A is not required by the GDPR or the SCCs, as the data importer does not need to submit the contract to its own government authority, unless the law of the country where the data importer is established requires it to do so prior to the transfer or disclosure of personal data5. Option B is not an obligation of the data importer, but of the data exporter, who must provide the data subjects with the information required by Articles 13 and 14 of the GDPR, including the fact that the data will be transferred to a third country and the appropriate safeguards in place6. Option C is not specific to the SCCs, but a general obligation of any controller or processor under the GDPR, who must cooperate with the supervisory authority and make available all information necessary to demonstrate compliance with their obligations7. Reference: 1: Article 46(1) of the GDPR 2: Standard Contractual Clauses (SCC) – European Commission 3: EU Standard Contractual Clauses (Word documents) 4: Clause 5(a) of the SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 5: Clause 5(b) of the SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 6: Clause 9 of the SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 7: Article 31 of the GDPR

Q150. 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 are ABC Hotel Chain and XYZ Travel Agency’s roles in this relationship?

* ABC Hotel Chain is the controller and XYZ Travel Agency is the processor.
* XYZ Travel Agency is the controller and ABC Hotel Chain is the processor.
* ABC Hotel Chain and XYZ Travel Agency are independent controllers.
* ABC Hotel Chain and XYZ Travel Agency are joint controllers.

Q151. Under Article 21 of the GDPR, a controller must stop profiling when requested by a data subject, unless it can demonstrate compelling legitimate grounds that override the interests of the individual. In the Guidelines on Automated individual decision-making and Profiling, the WP 29 says the controller needs to do all of the following to demonstrate that it has such legitimate grounds EXCEPT?
* Carry out an exercise that weighs the interests of the controller and the basis for the data subject’s objection.
* Consider the impact of the profiling on the data subject’s interest, rights and freedoms.
* Demonstrate that the profiling is for the purposes of direct marketing.
* Consider the importance of the profiling to their particular objective.

Reference https://gdpr-info.eu/art-21-gdpr/

Q152. With the issue of consent, the GDPR allows member states some choice regarding what?
* The mechanisms through which consent may be communicated
* The circumstances in which silence or inactivity may constitute consent
* The age at which children must be required to obtain parental consent
* The timeframe in which data subjects are allowed to withdraw their consent

Q153. Which of the following does NOT have to be included in the records most processors must maintain in relation to their data processing activities?
* Name and contact details of each controller on behalf of which the processor is acting.
* Categories of processing carried out on behalf of each controller for which the processor is acting.
* Details of transfers of personal data to a third country carried out on behalf of each controller for which the processor is acting.
* Details of any data protection impact assessment conducted in relation to any processing activities carried out by the processor on behalf of each controller for which the processor is acting.

Q154. SCENARIO

Please use the following to answer the next question:

T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.

T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze’s headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.

The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.

Which of the following is T-Craze’s lead supervisory authority?
* Germany, because that is where T-Craze is headquartered.
* France, because that is where T-Craze conducts processing of personal information.
* Spain, because that is T-Craze’s primary market based on its marketing campaigns.
* T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.

Q155. Company X has entrusted the processing of their payroll data to Provider Y.

Provider Y stores this encrypted data on its server. The IT department of Provider Y finds out that someone managed to hack into the system and take a copy of the data from its server. In this scenario, whom does Provider Y have the obligation to notify?
* The public
* Company X
* Law enforcement
* The supervisory authority

Q156. SCENARIO

Please use the following to answer the next question:

Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA.

Today, it is a multi-billion-dollar candy company operating in every continent. All of the company’s IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father’s company, but is also secretly working on launching a new global online dating website company called Ben Knows Best.

Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company’s online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers’ philosophical beliefs, political opinions and marital status.

If a customer identifies as single, Ben then copies all of that customer’s personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out.

Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.

Joe also hires his best friend’s daughter, Alice, who just graduated from law school in the U.S., to be the company’s new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company’s operations in the European Union to the U.S.

Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company’s IT

department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone’s information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.

In preparing the company for its impending lawsuit, Alice’s instruction to the company’s IT Department violated Article 5 of the GDPR because the company failed to first do what?
* Send out consent forms to all of its employees.
* Minimize the amount of data collected for the lawsuit.
* Inform all of its employees about the lawsuit.
* Encrypt the data from all of its employees.

Q157. How is the retention of communications traffic data for law enforcement purposes addressed by European data protection law?
* The ePrivacy Directive allows individual EU member states to engage in such data retention.
* The ePrivacy Directive harmonizes EU member states’ rules concerning such data retention.
* The Data Retention Directive’s annulment makes such data retention now permissible.
* The GDPR allows the retention of such data for the prevention, investigation, detection or prosecution of criminal offences only.

Q158. In the Planet 49 case, what was the main judgement of the Court of Justice of the European Union (CJEU) regarding the issue of cookies?
* If the cookies do not track personal data, then pre-checked boxes are acceptable.
* If the ePrivacy Directive requires consent for cookies, then the GDPR’s consent requirements apply.
* If a website’s cookie notice makes clear the information gathered and the lifespan of the cookie, then pre-checked boxes are acceptable.
* If a data subject continues to scroll through a website after reading a cookie banner, this activity constitutes valid consent for the tracking described in the cookie banner.

The CJEU ruled that the consent required by the ePrivacy Directive for the use of cookies must comply with the conditions laid down in the GDPR, which means that it must be specific, informed, unambiguous, and freely given. Therefore, pre-checked boxes or implied consent by scrolling are not valid forms of consent for cookies. The CJEU also clarified that the ePrivacy Directive applies to any information stored or accessed on a user’s device, regardless of whether it is personal data or not. Furthermore, the CJEU stated that the information provided to users about cookies must include the duration of the operation of cookies and the possibility of third parties accessing them.

Q159. 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 the required access.

How should the company respond to Jack’s request to be forgotten?
* The company should not erase the data at this time as it may be required to defend a legal claim of unfair dismissal.
* The company should erase all data relating to Jack without undue delay as the right to be forgotten is an absolute right.
* The company should claim that the right to be forgotten is not applicable to them, as only a fraction of their global workforce resides in the European Union.
* The company should ensure that the information is stored outside of the European Union so that the right to be forgotten under the GDPR does not apply.
According to the GDPR, the right to be forgotten, also known as the right to erasure, is not an absolute right and only applies in certain circumstances1. One of the exceptions to this right is when the processing of personal data is necessary for the establishment, exercise or defence of legal claims2. In this scenario, the company may need to retain the personal data of Jack, such as his employment records, performance reviews, and internal emails, in order to defend itself against a possible legal action of unfair dismissal. Therefore, the company should not erase the data at this time, unless it is confident that it has no legal basis to keep it. The company should also inform Jack of the reasons for not complying with his request and of his right to lodge a complaint with a supervisory authority or a judicial remedy3. Reference: 1: Everything you need to know about the “Right to be forgotten”2: Article 17(3)(e) of the GDPR3: Article 12(4) of the GDPR.

Q160. What must be included in a written agreement between the controller and processor in relation to processing conducted on the controller’s behalf?
* An obligation on the processor to report any personal data breach to the controller within 72 hours.
* An obligation on both parties to report any serious personal data breach to the supervisory authority.
* An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
* An obligation on the processor to assist the controller in complying with the controller’s obligations to notify the supervisory authority about personal data breaches.

Q161. In addition to the European Commission, who can adopt standard contractual clauses, assuming that all required conditions are met?
* Approved data controllers.
* The Council of the European Union.
* National data protection authorities.
* The European Data Protection Supervisor.
According to Article 46(2) of the GDPR, standard contractual clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) can be used as a legal basis for data transfers to third countries12. This means that, in addition to the European Commission, national data protection authorities can adopt standard contractual clauses, provided that they meet the conditions and requirements set out in the GDPR and obtain the approval of the Commission. The other options are not correct, as approved data controllers, the Council of the European Union and the European Data Protection Supervisor do not have the power to adopt standard contractual clauses under the GDPR. Reference: CIPP/E Certification – International Association of Privacy Professionals, Free CIPP/E Study Guide – International Association of Privacy Professionals, GDPR – EUR-Lex, Standard Contractual Clauses (SCC) – European Commission I hope this helps. If you have any other questions, please let me know.

Q162. How does the GDPR now define “processing”?
* Any act involving the collecting and recording of personal data.
* Any operation or set of operations performed on personal data or on sets of personal data.
* Any use or disclosure of personal data compatible with the purpose for which the data was collected.
* Any operation or set of operations performed by automated means on personal data or on sets of personal data.

Q163. If a multi-national company wanted to conduct background checks on all current and potential employees, including those based in Europe, what key provision would the company have to follow?

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