Vendor: IAPP

Exam Code: CIPP-E

Exam Name: Certified Information Privacy Professional/Europe (CIPP/E)

Version: DEMO

QUESTION 1
What type of data lies beyond the scope of the General Data Protection Regulation?

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

Answer: B
Explanation:
The General Data Protection Regulation (GDPR) is a data protection law that applies to the processing of personal data of individuals in the European Union (EU) and the European Economic Area (EEA). Personal data is any information relating to an identified or identifiable natural person, such as name, address, email, phone number, etc. The GDPR does not apply to personal data that is anonymized, meaning that it cannot be linked back to a specific individual. Anonymization can be achieved by removing or masking any identifying information from the data, such as using pseudonyms, aggregating or generalizing the data, or applying statistical methods. Therefore, the type of data that lies beyond the scope of the GDPR is anonymized data.

QUESTION 2
Under what circumstances would the GDPR apply to personal data that exists in physical form, such as information contained in notebooks or hard copy files?

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

Answer: D
Explanation:
The GDPR applies to all personal data, regardless of whether it exists in physical form or not. The GDPR defines personal data as any information relating to an identified or identifiable natural person, such as names, identification numbers, location data, or online identifiers. Therefore, any information that can be linked directly or indirectly to a natural person is considered personal data under the GDPR.
However, the GDPR also distinguishes between different types of processing activities and their legal bases. Processing activities are the operations performed on personal data, such as collection, storage, use, disclosure, or deletion. Processing activities can be either automated or manual. Automated processing means using technology to perform processing activities without human intervention. Manual processing means using human intervention to perform processing activities. The GDPR requires that any processing activity that involves personal data must comply with certain principles and conditions, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality. These principles and conditions apply to both automated and manual processing activities. Therefore, the GDPR applies to personal data that exists in physical form only when it is processed by an automated means in some way that affects its rights and freedoms. For example, if a company scans paper documents and stores them electronically in a database without deleting them after a certain period of time or when they are no longer needed for the original purpose for which they were collected (Article 6), then this would be considered an automated processing activity that involves personal data in physical form.

However, the GDPR does not apply to personal data that exists in physical form when it is handled in a sufficiently structured manner so as to form part of a filing system. For example, if a company keeps paper documents in folders labeled with names and dates on their office shelves without scanning them or storing them electronically anywhere else (Article 5), then this would not be considered an automated processing activity that involves personal data in physical form.

QUESTION 3
SCENARIO

Please use the following to answer the next question:

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

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

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

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

Why is this company obligated to comply with the GDPR?

A. The company has offices in the EU.
B. The company employs staff in the EU.
C. The company's data center is located in a country outside the EU.
D. The company's products are marketed directly to EU customers.

Answer: D
Explanation:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad

range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales. The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience. When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of home and have the character's abilities remain intact.

QUESTION 4
SCENARIO

Please use the following to answer the next question:

You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and AsiA. A large portion of the company's revenue is due to international sales. The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.

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

A. The NFC portal can read any data stored in the action figures
B. The information about the data processing involved has not been specified
C. The cloud service provider is in a country that has not been deemed adequate
D. The RFID tag in the action figures has the potential for misuse because of the toy's evolving capabilities

Answer: B
Explanation:
While all of the options present potential privacy issues, the lack of transparency about data processing poses the biggest risk for several reasons:
Uninformed Consent: Without clear information about data collection and usage, children and parents cannot make informed decisions about using the toys. This violates the principle of informed consent, which is a cornerstone of data protection laws. Hidden Features: The packaging and privacy policy do not disclose the hidden functionality of the toys, including the connection to the cloud and data processing in South Africa. This lack of transparency creates distrust and raises concerns about potential misuse of data. Unclear Data Flow: The explanation provided about the data flow is vague and incomplete. It is unclear what data is collected, how it is stored, for what purposes it is used, and who has access to it. This lack of clarity creates uncertainty and raises concerns about potential data breaches or leaks. Limited Control: Without detailed information about data practices, users have limited control over their information. They cannot opt out of data collection or request deletion of their data, further hindering their privacy rights.

QUESTION 5
SCENARIO

Please use the following to answer the next question:

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

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

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

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

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

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

Answer: D
Explanation:
According to Article 8 of the GDPR, where the processing of personal data is based on consent and the offer of an information society service (ISS) is directly made to a child, the processing is lawful only if the child is at least 16 years old, or if the consent is given or authorised by the holder of parental responsibility over the child. The GDPR allows EU member states to lower the age threshold to a minimum of 13 years. The data controller must make reasonable efforts to verify that the consent is given or authorised by the holder of parental responsibility, taking into account available technology. An ISS is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Examples of ISS include online marketplaces, social media platforms, and online games. In this scenario, the company is offering an ISS to children, as the connected toys can talk and interact with children via the internet. The company is also processing personal data of the children, such as their voice, questions, preferences, and location. Therefore, the company must obtain parental consent for the use of the action figures before any data can be collected, unless the child is above the age threshold set by the relevant EU member state. The company must also inform the parents and the children about the nature and purpose of the data processing, the data transfers to South Africa, and the rights of the data subjects. The company must also ensure that the data processing is fair, lawful, transparent, and in accordance with the data protection principles and the children's best interests.

QUESTION 6
SCENARIO

Please use the following to answer the next question:

You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and AsiA. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a QUESTION, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's QUESTION.
The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
In light of the requirements of Article 32 of the GDPR (related to the Security of Processing), which practice should the company institute?

A. Encrypt the data in transit over the wireless Bluetooth connection.
B. Include dual-factor authentication before each use by a child in order to ensure a minimum amount of security.
C. Include three-factor authentication before each use by a child in order to ensure the best level of security possible.
D. Insert contractual clauses into the contract between the toy manufacturer and the cloud service provider, since South Africa is outside the European Union.

Answer: A
Explanation:
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.

QUESTION 7
Which of the following would most likely NOT be covered by the definition of "personal data" under the GDPR?

A. The payment card number of a Dutch citizen
B. The U.S. social security number of an American citizen living in France
C. The unlinked aggregated data used for statistical purposes by an Italian company
D. The identification number of a German candidate for a professional examination in Germany

Answer: C
Explanation:
The definition of personal data under the GDPR is broad and covers any information that relates to an identified or identifiable natural person. This means that personal data can include information such as name, email, phone number, address, date of birth, race, gender, political opinions and more. The GDPR protects personal data on all levels, platforms and technologies, and requires organizations to process it only for a specific purpose and keep it for a limited time.
The unlinked aggregated data used for statistical purposes by an Italian company would most likely NOT be covered by the definition of personal data under the GDPR. Aggregated data is data that has been processed in such a way that individual records are no longer identifiable. For example, if a company collects the names and email addresses of its customers and then calculates the average age of its customers, the resulting data is aggregated and not personal. Therefore, this type of data would not be subject to the GDPR.
However, this does not mean that the Italian company can use this type of data without any restrictions or obligations. The GDPR still applies to any processing activity that involves personal data in any form or manner. For example, if the Italian company uses this type of data to create a profile or a segment of its customers based on their characteristics or preferences, it may still need to comply with certain principles and conditions under the GDPR. For instance, it may need to obtain consent from its customers before using their aggregated data for marketing purposes; it may need to ensure that its aggregated data is accurate and up-to-date; it may need to limit the retention period of its aggregated data; and it may need to respect the rights of its customers regarding their personal data.

QUESTION 8
Which of the following would MOST likely trigger the extraterritorial effect of the GDPR, as specified by Article 3?

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

Answer: B

Explanation:
According to Article 3(1) of the GDPR1, personal data shall be processed in any member state only on the basis of a decision taken at a Union level that is binding for that member state, unless it is derogated from by national law. This means that the GDPR applies to any processing of personal data within the EU, regardless of where the controller or processor is located, as long as it is based on a decision made at a Union level that is binding for that member state. Therefore, option B would most likely trigger the extraterritorial effect of the GDPR, as it involves personal data of EU citizens being processed by a controller or processor based outside the EU, which may be subject to a decision made at a Union level that is binding for that member state. Option A would not trigger the extraterritorial effect of the GDPR, as it involves monitoring suspected terrorists, which is not considered processing under Article 4(1) and (2) of the GDPR. Monitoring may fall under other legal frameworks, such as national security or counter-terrorism laws. Option C would not trigger the extraterritorial effect of the GDPR, as it involves monitoring EU citizens outside the EU by non-EU law enforcement bodies, which may not be subject to any decision made at a Union level that is binding for that member state. Option D would not trigger the extraterritorial effect of the GDPR, as it involves processing personal data of EU residents by a non-EU business that targets EU customers, which may not be subject to any decision made at a Union level that is binding for that member state.

QUESTION 9
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: B
Explanation:
The GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4(2)). This is a broad definition that covers almost any activity involving personal data, regardless of the method or means used. The GDPR also specifies that processing should be lawful, fair and transparent, and should respect the principles of data protection by design and by default (Article 5).

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

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

Answer: C
Explanation:
According to the UK GDPR, a processor is a natural or legal person, public authority, agency or

other body which processes personal data on behalf of the controller. A processor must act only on the documented instructions of the controller and must not process the data for its own purposes or in a way that is incompatible with the controller's purposes. If a processor makes an independent decision regarding the purposes and means of processing it carries out on behalf of a controller, it will be considered to be a controller in respect of that processing and will be subject to the same obligations and liabilities as a controller under the UK GDPR. This means that the processor will have to comply with the data protection principles, ensure the rights of data subjects, implement appropriate technical and organisational measures, report data breaches, conduct data protection impact assessments, appoint a data protection officer if required, and cooperate with the supervisory authority. The processor will also be exposed to the risk of administrative fines, compensation claims, and reputational damage.

QUESTION 11
According to the GDPR, how is pseudonymous personal data defined?

A. Data that can no longer be attributed to a specific data subject without the use of additional information kept separately.
B. Data that can no longer be attributed to a specific data subject, with no possibility of re-identifying the data.
C. Data that has been rendered anonymous in such a manner that the data subject is no longer identifiable.
D. Data that has been encrypted or is subject to other technical safeguards.

Answer: A
Explanation:
Pseudonymisation is a technique that replaces, removes or transforms information that identifies individuals, and keeps that information separate from the rest of the data. Pseudonymised data is still personal data under the GDPR, because it can be re-identified with the use of additional information. However, pseudonymisation can reduce the risks of processing personal data and help comply with data protection principles and obligations. Pseudonymisation is different from anonymisation, which is the process of irreversibly transforming personal data so that the data subject is no longer identifiable.

QUESTION 12
Under which of the following conditions does the General Data Protection Regulation NOT apply to the processing of personal data?

A. When the personal data is processed only in non-electronic form
B. When the personal data is collected and then pseudonymised by the controller
C. When the personal data is held by the controller but not processed for further purposes
D. When the personal data is processed by an individual only for their household activities

Answer: D
Explanation:
The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. However, the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. This means that individuals can process personal data without being subject to the GDPR, as long as the processing is not related to a professional or commercial activity. For example, the GDPR does not apply to an individual who keeps a personal address book or who posts photos of their family and friends on a social media platform, as long as the platform is not used for business purposes.

QUESTION 13
According to the E-Commerce Directive 2000/31/EC, where is the place of "establishment" for a company providing services via an Internet website confirmed by the GDPR?

A. Where the technology supporting the website is located
B. Where the website is accessed
C. Where the decisions about processing are made
D. Where the customer's Internet service provider is located

Answer: C
Explanation:
According to the E-Commerce Directive 2000/31/EC, the place of establishment for a company providing services via an Internet website is the place where the service provider effectively pursues an economic activity through a fixed establishment for an indefinite period of time. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider. The place of establishment is determined by the place where the decisions about processing are made, not by the place where the technology supporting the website is located, where the website is accessed, or where the customer's Internet service provider is located. This is confirmed by the GDPR, which applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.

QUESTION 14
SCENARIO

Please use the following to answer the next question:
Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance. Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.
In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes. Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.
In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data

being used by them in any way.
Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.
Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system. Which statement accurately summarizes Bedrock's obligation in regard to Louis's data portability request?

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

Answer: B

QUESTION 15
SCENARIO

Please use the following to answer the next question:

Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.

Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.

In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.

Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.

After Louis has exercised his right to restrict the use of his data, under what conditions would Accidentable have grounds for refusing to comply?

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

Answer: A

QUESTION 16
Under the GDPR, who would be LEAST likely to be allowed to engage in the collection, use, and disclosure of a data subject's sensitive medical information without the data subject's knowledge or consent?

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

Answer: D
Explanation:
The GDPR defines data concerning health as a special category of personal data that is subject to specific processing conditions and safeguards. The GDPR prohibits the processing of such data unless one of the exceptions in Article 9 applies. One of these exceptions is the explicit consent of the data subject, which means that the data subject has given a clear and affirmative indication of their agreement to the processing of their health data. Another exception is when the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care. A third exception is when the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. These exceptions are based on the principle of necessity, which means that the processing must be strictly necessary for a specific purpose and

cannot be achieved by other means. In the given scenario, the journalist does not fall under any of these exceptions. The journalist is not a health professional, a public authority, or a person who has obtained the explicit consent of the data subject. The journalist is not processing the data for any legitimate purpose related to public health, medical care, or social protection. The journalist is merely pursuing their own interest in publishing a story that may or may not be in the public interest. The journalist is not respecting the data subject's rights and freedoms, especially their right to privacy and confidentiality. Therefore, the journalist would be least likely to be allowed to engage in the collection, use, and disclosure of the data subject's sensitive medical information without their knowledge or consent.

QUESTION 17
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
Explanation:
The GDPR states that the parental consent mechanism generally applies when the child is younger than 16 years. Processing personal data will be lawful only if the child's parent or custodian has consented to such processing. However, Member States are allowed to lower this threshold in national legislation up to 13 years old. This means that Member States have some choice regarding the age limit for children's consent, as long as it is not below 13 years. The GDPR also requires that the consent request is clear and understandable for the child, and that the controller makes reasonable efforts to verify that the consent is given or authorised by the holder of parental responsibility.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**