# Topic 1 - Exam A

Question #1 Topic 1

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

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



Question #2 Topic 1

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

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

Reveal Solution Discussion

Question #3 Topic 1

A key component of the OECD Guidelines is the "Individual Participation Principle". What parts of the General Data Protection Regulation (GDPR) provide the closest equivalent to that principle?

- A. The lawful processing criteria stipulated by Articles 6 to 9
- B. The information requirements set out in Articles 13 and 14
- C. The breach notification requirements specified in Articles 33 and 34
- D. The rights granted to data subjects under Articles 12 to 22

Reveal Solution Discussion 2

Question #4 Topic 1

A. The European Council

B. The European Parliament

C. The European Commission

D. The Council of the European Union

Question #5 Topic 1

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?

- A. ECHR can rule on issues concerning privacy as a fundamental right, while the CJEU cannot.
- B. CJEU can force national governments to implement and honor EU law, while the ECHR cannot.
- C. CJEU can hear appeals on human rights decisions made by national courts, while the ECHR cannot.
- D. ECHR can enforce human rights laws against governments that fail to implement them, while the CJEU cannot.

Reveal Solution Discussion 1

Discussion 2

Question #6 Topic 1

# SCENARIO -

**Reveal Solution** 

Please use the following to answer the next question:

Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:

Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.

Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).

Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees. These records are available to former students after registering through Granchester's Alumni portal.

Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.

Under their security policy, the University encrypts all of its personal data records in transit and at rest.

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

One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs Anna about his performance database.

Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.

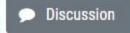
Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop

into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.

Which of the University's records does Anna NOT have to include in her record of processing activities?

- A. Student records
- B. Staff and alumni records
- C. Frank's performance database
- D. Department for Education records

**Reveal Solution** 



Question #7 Topic 1

# SCENARIO -

Please use the following to answer the next question:

Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:

Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.

Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).

Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees. These records are available to former students after registering through Granchester's Alumni portal.

Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.

Under their security policy, the University encrypts all of its personal data records in transit and at rest.

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

One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs Anna about his performance database.

Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.

Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.

Before Anna determines whether Frank's performance database is permissible, what additional information does she need?

- A. More information about Frank's data protection training.
- B. More information about the extent of the information loss.
- C. More information about the algorithm Frank used to mask student numbers.
- D. More information about what students have been told and how the research will be used.

Reveal Solution Discussion 5

Question #8 Topic 1

## SCENARIO -

Please use the following to answer the next question:

Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:

Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.

Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).

Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees. These records are available to former students after registering through Granchester's Alumni portal.

Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.

Under their security policy, the University encrypts all of its personal data records in transit and at rest.

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

One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs Anna about his performance database.

Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.

Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train. Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.

Anna will find that a risk analysis is NOT necessary in this situation as long as?

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

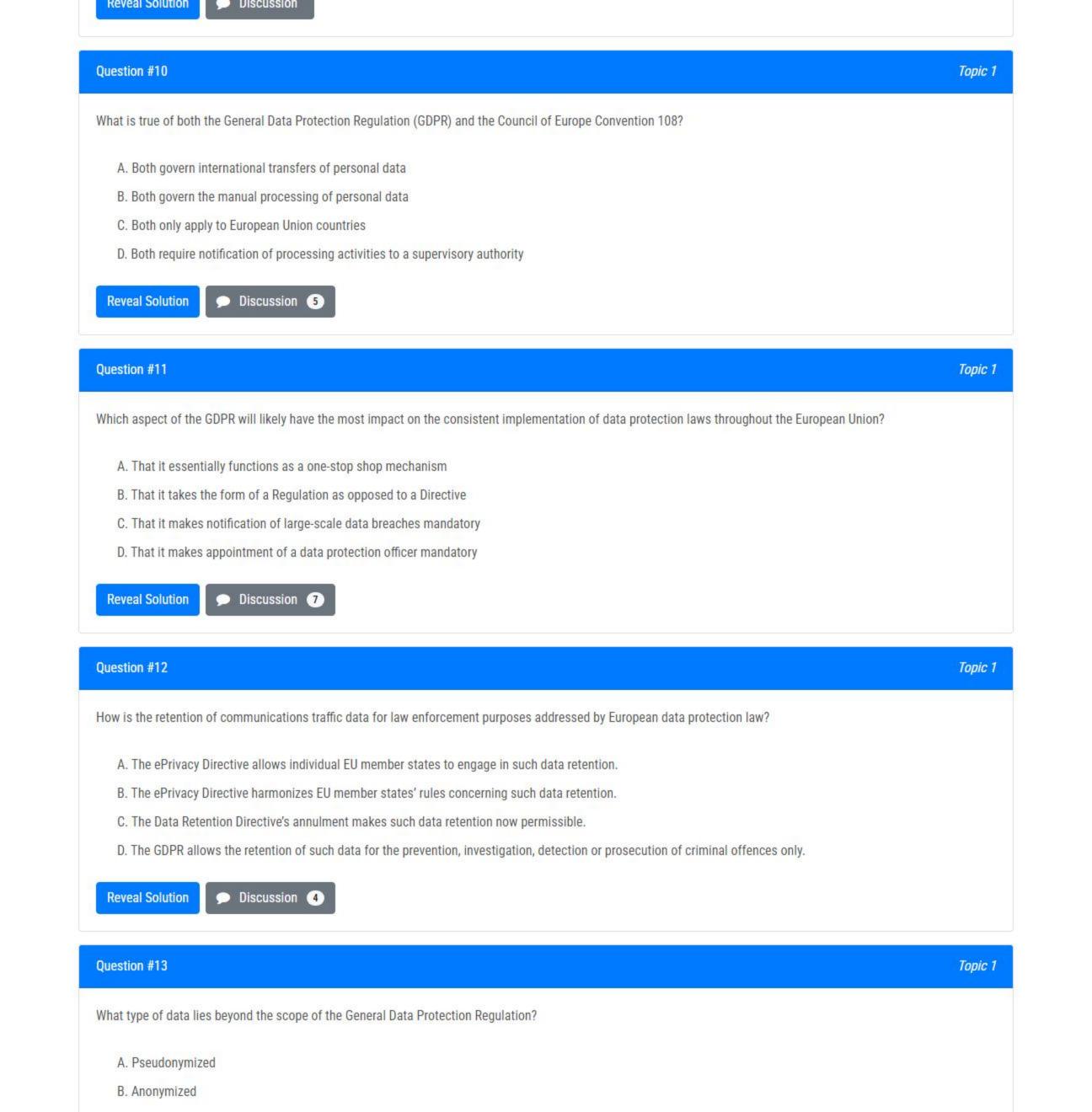
Reveal Solution

Discussion

Question #9 Topic 1

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

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



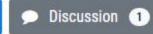


Question #14 Topic 1

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.

Reveal Solution



Question #15 Topic 1

#### 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.

Reveal Solution Discussion

Question #16 Topic 1

## 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.

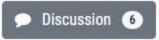
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. 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

Reveal Solution



Question #17 Topic 1

# 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.

**Reveal Solution** 

Discussion

**Question #18** Topic 1

#### 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.

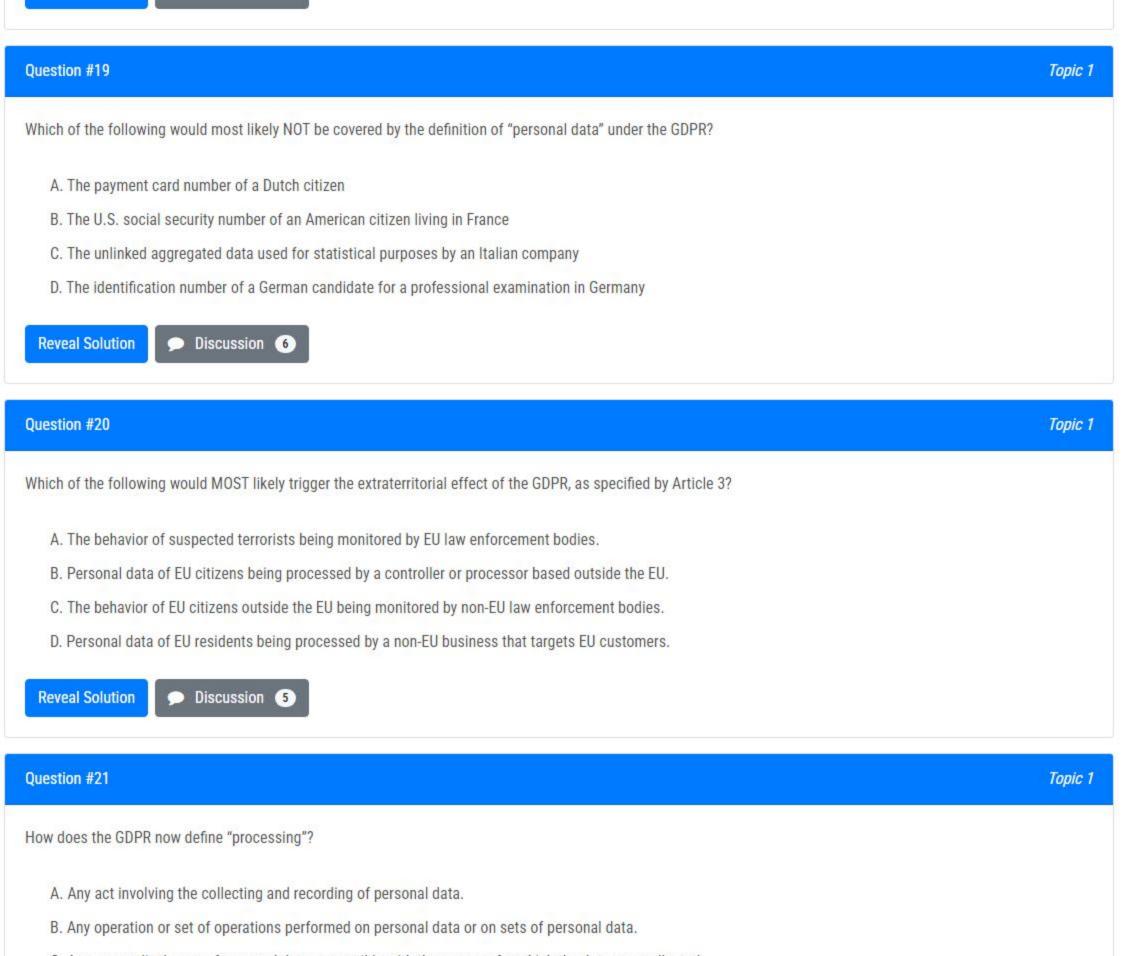
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. 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.



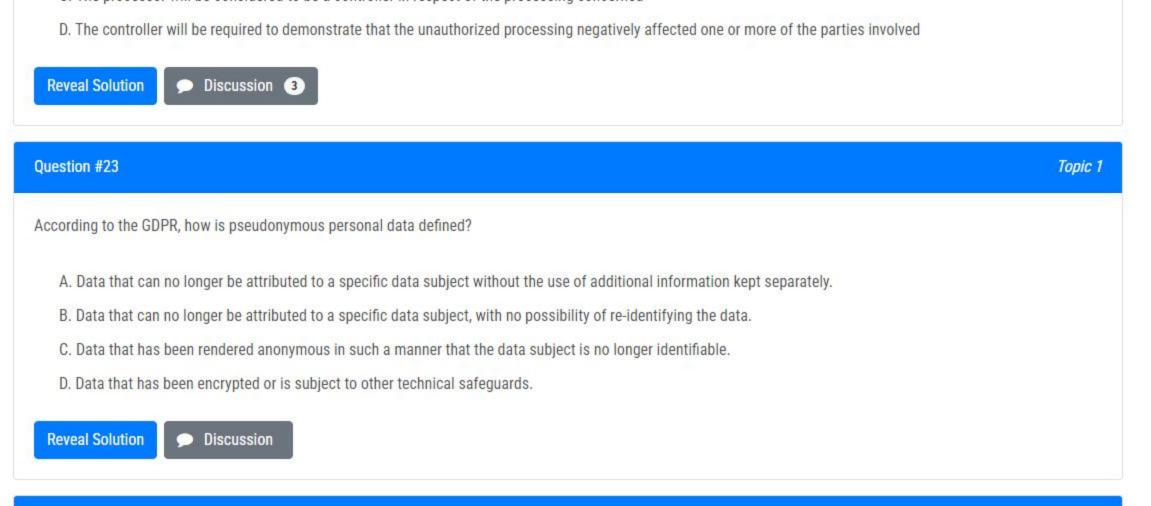


C. Any use or disclosure of personal data compatible with the purpose for which the data was collected. D. Any operation or set of operations performed by automated means on personal data or on sets of personal data. Discussion **Reveal Solution** 

Question #22 Topic 1

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



Question #24 Topic 1

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

Reveal Solution Discussion 8

Question #25 Topic 1

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

Reveal Solution Discussion

Question #26 Topic 1

## SCENARIO -

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.

Reveal Solution



Question #27 Topic 1

#### 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.

**Reveal Solution** 

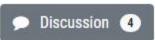


Question #28 Topic 1

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.

**Reveal Solution** 



Question #29 Topic 1

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

**Reveal Solution** 



Question #30 Topic 1

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

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



Question #31 Topic 1

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

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



Question #32 Topic 1

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

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

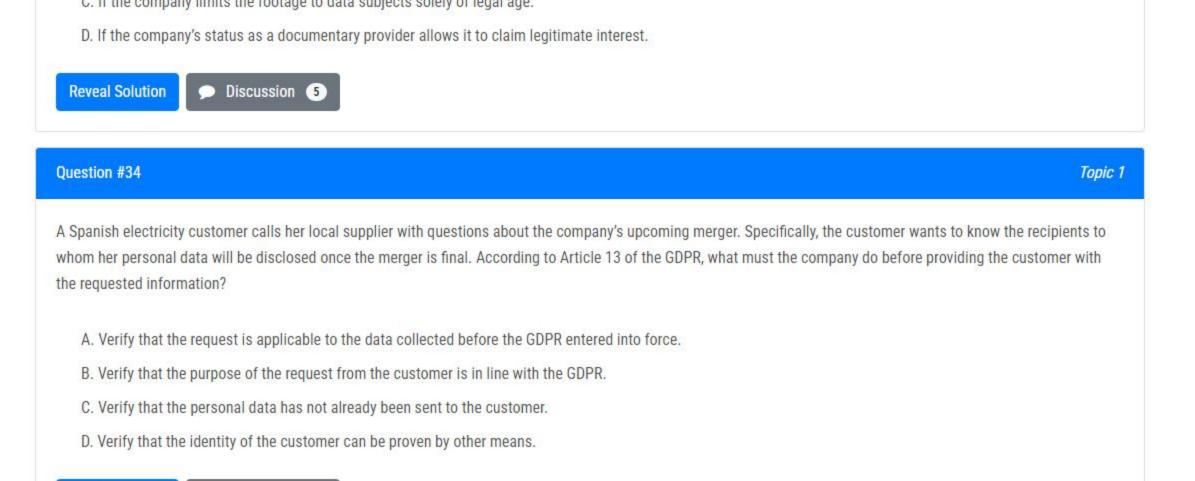
Reveal Solution 

Discussion

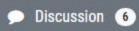
Question #33 Topic 1

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

- A. If obtaining consent is deemed to involve disproportionate effort.
- B. If obtaining consent is deemed voluntary by local legislation.



Reveal Solution

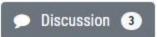


Question #35 Topic 1

Under the GDPR, where personal data is not obtained directly from the data subject, a controller is exempt from directly providing information about processing to the data subject if?

- A. The data subject already has information regarding how his data will be used
- B. The provision of such information to the data subject would be too problematic
- C. Third-party data would be disclosed by providing such information to the data subject
- D. The processing of the data subject's data is protected by appropriate technical measures

Reveal Solution



Question #36 Topic 1

SCENARIO -

Please use the following to answer the next question:

Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.

Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service.

Company B's live systems will contain the following information for each of Company A's employees:

Name -

Address -

Date of Birth -

National Insurance number -	
Sick pay entitlement -	
Maternity/paternity pay entitlement	
Holiday entitlement -	
Pension and benefits contributions	
Trade union contributions -	
Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment and attendance system, but isn't sure whether or not this is required.	nent in relation to the new time
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attenda	ance data only for the purpose
of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny so obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign of the contract o	suggests that Company B
Company A enters into the contract.	
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of	
engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data process	an ma <sup>te</sup> it is a larger to
agreement, as data is only being used for IT testing purposes.	
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of	
letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she n	Annahara and Annahara and Annahara
Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?	ounce an arrested employees.
A. Their omission of data protection provisions in their contract with Company C.	
B. Their failure to provide sufficient security safeguards to Company A's data.	
C. Their engagement of Company C to improve their payroll service.	
D. Their decision to operate without a data protection officer.	
Reveal Solution Discussion	
Question #37	Topic 1
SCENARIO -	
Please use the following to answer the next question:	
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll function to Company B. Company B. Company B. an established payroll function to Company B. Company B. an established payroll function to Company B. Company B. an established payroll function to Company B. Company B. an established payroll function to Company B. Company B. an established payroll function to Company B. Company B. an established payroll function to Company B. Company B. an established payroll function to Company B. and the company B	payroll service provider with a
sizable client base and a solid reputation in the industry.	
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system inst	
factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to prove	ide the payroll service.
Company B's live systems will contain the following information for each of Company A's employees:	
Name -	
Address -	
Date of Birth -	
Payroll number -	
1 dyron number	

Payroll number -

National Insurance number -

Sick pay entitlement -

Maternity/paternity pay entitlement

Holiday entitlement -

Pension and benefits contributions

Trade union contributions -

Jenny is the compliance officer at Company A. She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.

Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.

Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B. This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.

Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she notifies all affected employees. The GDPR requires sufficient guarantees of a company's ability to implement adequate technical and organizational measures. What would be the most realistic way that Company B could have fulfilled this requirement?

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

Reveal Solution Discussion 2

Question #38 Topic 1

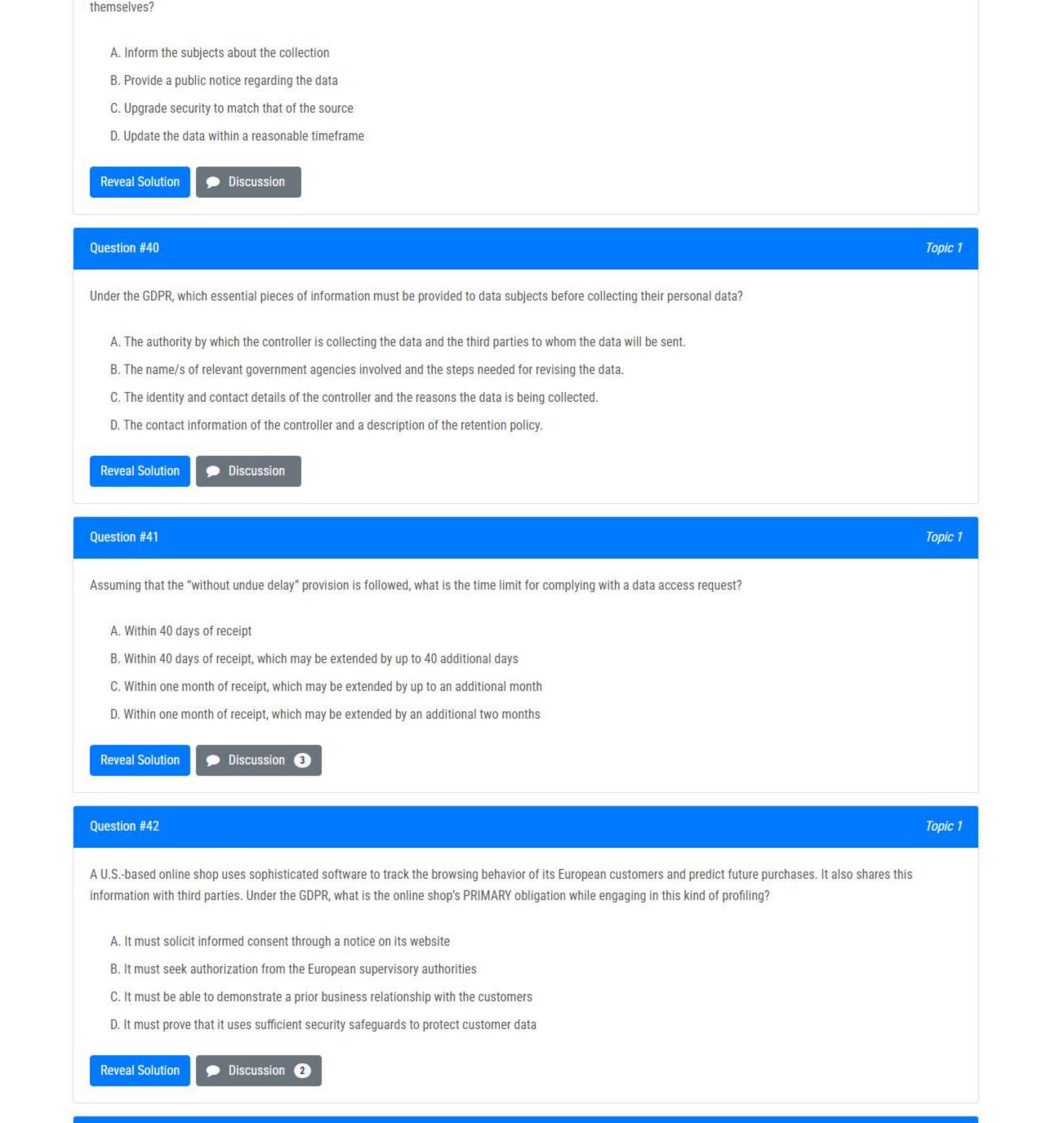
In 2016's Guidance, the United Kingdom's Information Commissioner's Office (ICO) reaffirmed the importance of using a "layered notice" to provide data subjects with what?

- A. A privacy notice containing brief information whilst offering access to further detail.
- B. A privacy notice explaining the consequences for opting out of the use of cookies on a website.
- C. An explanation of the security measures used when personal data is transferred to a third party.
- D. An efficient means of providing written consent in member states where they are required to do so.

Reveal Solution Discussion

Question #39 Topic 1

When collecting personal data in a European Union (EU) member state, what must a company do if it collects personal data from a source other than the data subjects

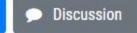


Question #43 Topic 1

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

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

Reveal Solution



Question #44 Topic 1

Under Article 21 of the GDPR, a controller must stop profiling when requested by a data subject, unless it can demonstrate compelling legitimate grounds that override the interests of the individual. In the Guidelines on Automated individual decision-making and Profiling, the WP 29 says the controller needs to do all of the following to demonstrate that it has such legitimate grounds EXCEPT?

- A. Carry out an exercise that weighs the interests of the controller and the basis for the data subject's objection.
- B. Consider the impact of the profiling on the data subject's interest, rights and freedoms.
- C. Demonstrate that the profiling is for the purposes of direct marketing.
- D. Consider the importance of the profiling to their particular objective.

**Reveal Solution** 



Question #45 Topic 1

## SCENARIO -

Please use the following to answer the next question:

TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.

During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.

If TripBliss Inc. decides not to report the incident to the supervisory authority, what would be their BEST defense?

- A. The resulting obligation to notify data subjects would involve disproportionate effort.
- B. The incident resulted from the actions of a third-party that were beyond their control.
- C. The destruction of the stolen data makes any risk to the affected data subjects unlikely.
- D. The sensitivity of the categories of data involved in the incident was not substantial enough.



Question #46 Topic 1

### SCENARIO -

Please use the following to answer the next question:

TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.

During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.

With regard to TripBliss Inc.'s use of website cookies, which of the following statements is correct?

- A. Because not all of the cookies are strictly necessary to enable the use of a service requested from TripBliss Inc., consent requirements apply to their use of cookies.
- B. Because of the categories of data involved, explicit consent for the use of cookies must be obtained separately from customers.
- C. Because Techiva will receive only aggregate statistics of data collected from the cookies, no additional consent is necessary.
- D. Because the use of cookies involves the potential for location tracking, explicit consent must be obtained from customers.

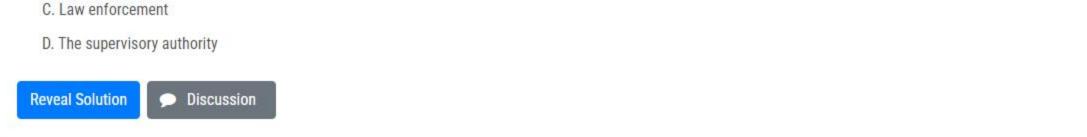
Reveal Solution

Discussion

Question #47 Topic 1

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?

- A. The public
- B. Company X





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

A. A postal notification

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

Discussion 3

**Reveal Solution** 



Question #50 Topic 1

Which of the following would require designating a data protection officer?

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

Reveal Solution Discussion

Question #51 Topic 1

Which of the following describes a mandatory requirement for a group of undertakings that wants to appoint a single data protection officer?

- A. The group of undertakings must obtain approval from a supervisory authority.
- B. The group of undertakings must be comprised of organizations of similar sizes and functions.
- C. The data protection officer must be located in the country where the data controller has its main establishment.
- D. The data protection officer must be easily accessible from each establishment where the undertakings are located.



Question #52 Topic 1

What obligation does a data controller or processor have after appointing a data protection officer?

- A. To ensure that the data protection officer receives sufficient instructions regarding the exercise of his or her defined tasks.
- B. To provide resources necessary to carry out the defined tasks of the data protection officer and to maintain his or her expert knowledge.
- C. To ensure that the data protection officer acts as the sole point of contact for individuals' questions about their personal data.
- D. To submit for approval to the data protection officer a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.

Reveal Solution

Discussion

Question #53 Topic 1

### SCENARIO -

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketlQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketlQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketlQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she

For what reason would JaphSoft be considered a controller under the GDPR?

- A. It determines how long to retain the personal data collected.
- B. It has been provided access to personal data in the MarketIQ database.
- C. It uses personal data to improve its products and services for its client-base through machine learning.
- D. It makes decisions regarding the technical and organizational measures necessary to protect the personal data.

**Reveal Solution** 



Question #54 Topic 1

## SCENARIO -

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketlQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketlQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

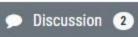
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketlQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.

Why would the consent provided by Ms. Iman NOT be considered valid in regard to JaphSoft?

- A. She was not told which controller would be processing her personal data.
- B. She only viewed the visual representations of the privacy notice Liem provided.
- C. She did not read the privacy notice stating that her personal data would be shared.
- D. She has never made any purchases from JaphSoft and has no relationship with the company.

**Reveal Solution** 



Question #55 Topic 1

## SCENARIO -

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the

same marketing database, MarketIQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketlQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

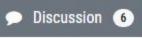
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketlQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.

JaphSoft's use of pseudonymization is NOT in compliance with the CDPR because?

- A. JaphSoft failed to first anonymize the personal data.
- B. JaphSoft pseudonymized all the data instead of deleting what it no longer needed.
- C. JaphSoft was in possession of information that could be used to identify data subjects.
- D. JaphSoft failed to keep personally identifiable information in a separate database.

Reveal Solution



Question #56 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketlQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketlQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketlQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.

Which of the following BEST describes the relationship between Liem, EcoMick and JaphSoft?

- A. Liem is a controller and EcoMick is a processor because Liem provides specific instructions regarding how the marketing campaigns should be rolled out.
- B. EcoMick and JaphSoft are is a controller and Liem is a processor because EcoMick is sharing its marketing data with Liem for contacts in Europe.



D. Liem and EcoMick are joint controllers because they carry out joint marketing activities.



Question #57 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Discussion

Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketlQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.

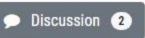
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.

Under its agreement with Liem and EcoMick, JaphSoft received access to MarketlQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.

Under the GDPR, Liem and EcoMick's contract with MarketIQ must include all of the following provisions EXCEPT?

- A. Processing the personal data upon documented instructions regarding data transfers outside of the EEA.
- B. Notification regarding third party requests for access to Liem and EcoMick's personal data.
- C. Assistance to Liem and EcoMick in their compliance with data protection impact assessments.
- D. Returning or deleting personal data after the end of the provision of the services.

Reveal Solution

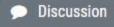


Question #58 Topic 1

When is data sharing agreement MOST likely to be needed?

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

Reveal Solution



Question #59 Topic 1

An employee of company ABCD has just noticed a memory stick containing records of client data, including their names, addresses and full contact details has disappeared. The data on the stick is unencrypted and in clear text. It is uncertain what has happened to the stick at this stage, but it likely was lost during the travel of an employee. What should the company do?

- A. Notify as soon as possible the data protection supervisory authority that a data breach may have taken place.
- B. Launch an investigation and if nothing is found within one month, notify the data protection supervisory authority.
- C. Invoke the "disproportionate effort" exception under Article 33 to postpone notifying data subjects until more information can be gathered.
- D. Immediately notify all the customers of the company that their information has been accessed by an unauthorized person.

**Reveal Solution** 

Discussion

Question #60 Topic 1

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

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

Reveal Solution

Discussion

Question #61 Topic 1

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

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

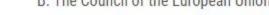
**Reveal Solution** 

Discussion 6

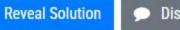
Question #62 Topic 1

In addition to the European Commission, who can adopt standard contractual clauses, assuming that all required conditions are met?

- A. Approved data controllers.



- C. National data protection authorities.
- D. The European Data Protection Supervisor.



Discussion 5

Question #63 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland.

Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.

The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.

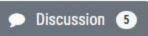
In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures, Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.

What would MOST effectively assist Zandelay in conducting their data protection impact assessment?

- A. Information about DPIAs found in Articles 38 through 40 of the GDPR.
- B. Data breach documentation that data controllers are required to maintain.
- C. Existing DPIA guides published by local supervisory authorities.
- D. Records of processing activities that data controllers are required to maintain.

Reveal Solution



Question #64 Topic 1

# SCENARIO -

Please use the following to answer the next question:

Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland.

Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.

The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.

In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures. Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.

What would Zandalay assists to the assessite on eath ority during the paint assessitation?

A. An evaluation of the complexity of the intended processing.

B. An explanation of the purposes and means of the intended processing.

C. Records showing that customers have explicitly consented to the intended profiling activities.



Question #65 Topic 1

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

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

D. Certificates that prove Martin's professional qualities and expert knowledge of data protection law.

Reveal Solution Discussion

Question #66 Topic 1

Which of the following countries will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary?

- A. Greece
- B. Norway
- C. Australia
- D. Switzerland

Reveal Solution Discussion 3

Question #67 Topic 1

A company is hesitating between Binding Corporate Rules and Standard Contractual Clauses as a global data transfer solution. Which of the following statements would help the company make an effective decision?

- A. Binding Corporate Rules are especially recommended for small and medium companies.
- B. The data exporter does not need to be located in the EU for the standard Contractual Clauses.
- C. Binding Corporate Rules provide a global solution for all the entities of a company that are bound by the intra-group agreement.
- D. The company will need the prior authorization of all EU data protection authorities for concluding Standard Contractual Clauses.

Reveal Solution

Discussion

Question #68 Topic 1

Under the GDPR, which of the following is true in regard to adequacy decisions involving cross-border transfers?

- A. The European Commission can adopt an adequacy decision for individual companies.
- B. The European Commission can adopt, repeal or amend an existing adequacy decision.
- C. EU member states are vested with the power to accept or reject a European Commission adequacy decision.
- D. To be considered as adequate, third countries must implement the EU General Data Protection Regulation into their national legislation.



Question #69 Topic 1

Under Article 58 of the GDPR, which of the following describes a power of supervisory authorities in European Union (EU) member states?

- A. The ability to enact new laws by executive order.
- B. The right to access data for investigative purposes.
- C. The discretion to carry out goals of elected officials within the member state.
- D. The authority to select penalties when a controller is found guilty in a court of law.



Question #70 Topic 1

# SCENARIO -

Please use the following to answer the next question:

Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.

Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.

Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.

Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?

A. Submit a draft decision to other supervisory authorities for their opinion.

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



Question #71 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.

Javier contacts the U.K. Information Commissioner's Office ('ICO' – the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.

Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website. Assuming that multiple EVETFIT branches across several EU countries are acting as separate data controllers, and that each of those branches were responsible for mishandling Javier's request, how may Javier proceed in order to seek compensation?

- A. He will have to sue the EVETFIT's head office in France, where EVETFIT has its main establishment.
- B. He will be able to sue any one of the relevant EVETFIT branches, as each one may be held liable for the entire damage.
- C. He will have to sue each EVETFIT branch so that each branch provides proportionate compensation commensurate with its contribution to the damage or distress suffered by Javier.
- D. He will be able to apply to the European Data Protection Board in order to determine which particular EVETFIT branch is liable for damages, based on the decision that was made by the board.

Reveal Solution Discussion 2

Question #72 Topic 1

The GDPR specifies fines that may be levied against data controllers for certain infringements. Which of the following infringements would be subject to the less severe administrative fine of up to 10 million euros (or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year)?

- A. Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing.
- B. Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default.
- C. Failure to process personal information in a manner compatible with its original purpose.
- D. Failure to provide the means for a data subject to rectify inaccuracies in personal data.

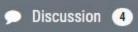


Question #73 Topic 1

What is the MAIN reason GDPR Article 4(22) establishes the concept of the "concerned supervisory authority"?

- A. To encourage the consistency of local data processing activity.
- B. To give corporations a choice about who their supervisory authority will be.
- C. To ensure the GDPR covers controllers that do not have an establishment in the EU but have a representative in a member state.
- D. To ensure that the interests of individuals residing outside the lead authority's jurisdiction are represented.

**Reveal Solution** 



Question #74 Topic 1

Which area of privacy is a lead supervisory authority's (LSA) MAIN concern?

- A. Data subject rights
- B. Data access disputes
- C. Cross-border processing
- D. Special categories of data

**Reveal Solution** 

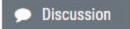


Question #75 Topic 1

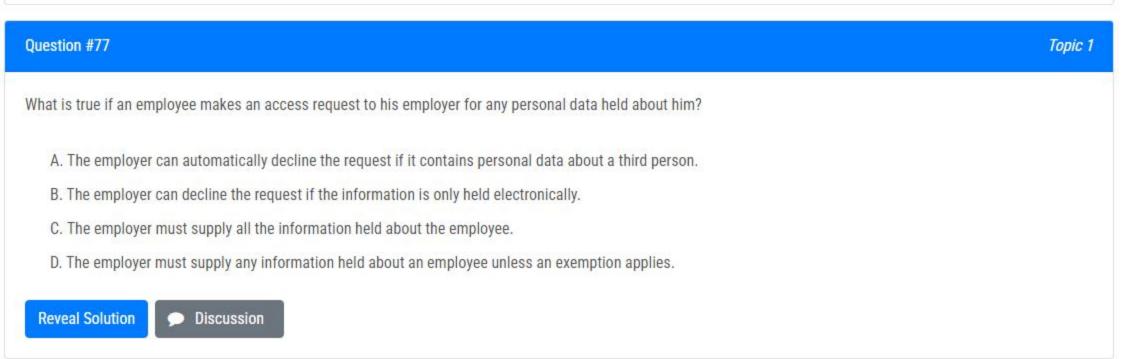
If a multi-national company wanted to conduct background checks on all current and potential employees, including those based in Europe, what key provision would the company have to follow?

- A. Background checks on employees could be performed only under prior notice to all employees.
- B. Background checks are only authorized with prior notice and express consent from all employees including those based in Europe.
- C. Background checks on European employees will stem from data protection and employment law, which can vary between member states.
- D. 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.

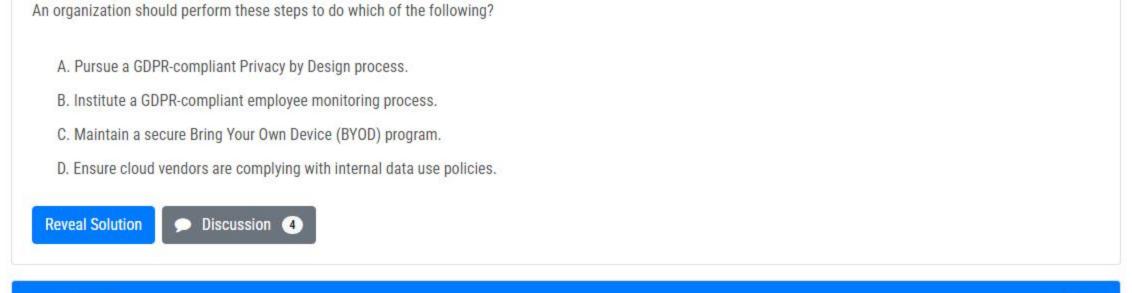
**Reveal Solution** 







# Read the following steps: Discover which employees are accessing cloud services and from which devices and apps Lock down the data in those apps and devices Monitor and analyze the apps and devices for compliance Manage application life cycles Monitor data sharing -





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

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

Reveal Solution Discussion 7

Question #80 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.

Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.

To comply with the GDPR, what should Building Block have done as a first step before implementing the SecurityScan measure?

- A. Assessed potential privacy risks by conducting a data protection impact assessment.
- B. Consulted with the relevant data protection authority about potential privacy violations.
- C. Distributed a more comprehensive notice to employees and received their express consent.
- D. Consulted with the Information Security team to weigh security measures against possible server impacts.

**Reveal Solution** 



Question #81 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.

Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.

What would be the MOST APPROPRIATE way for Building Block to handle the situation with the employee from Italy?

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



Question #82 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

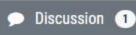
After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.

Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.

In addition to notifying employees about the purpose of the monitoring, the potential uses of their data and their privacy rights, what information should Building Block have provided them before implementing the security measures?

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

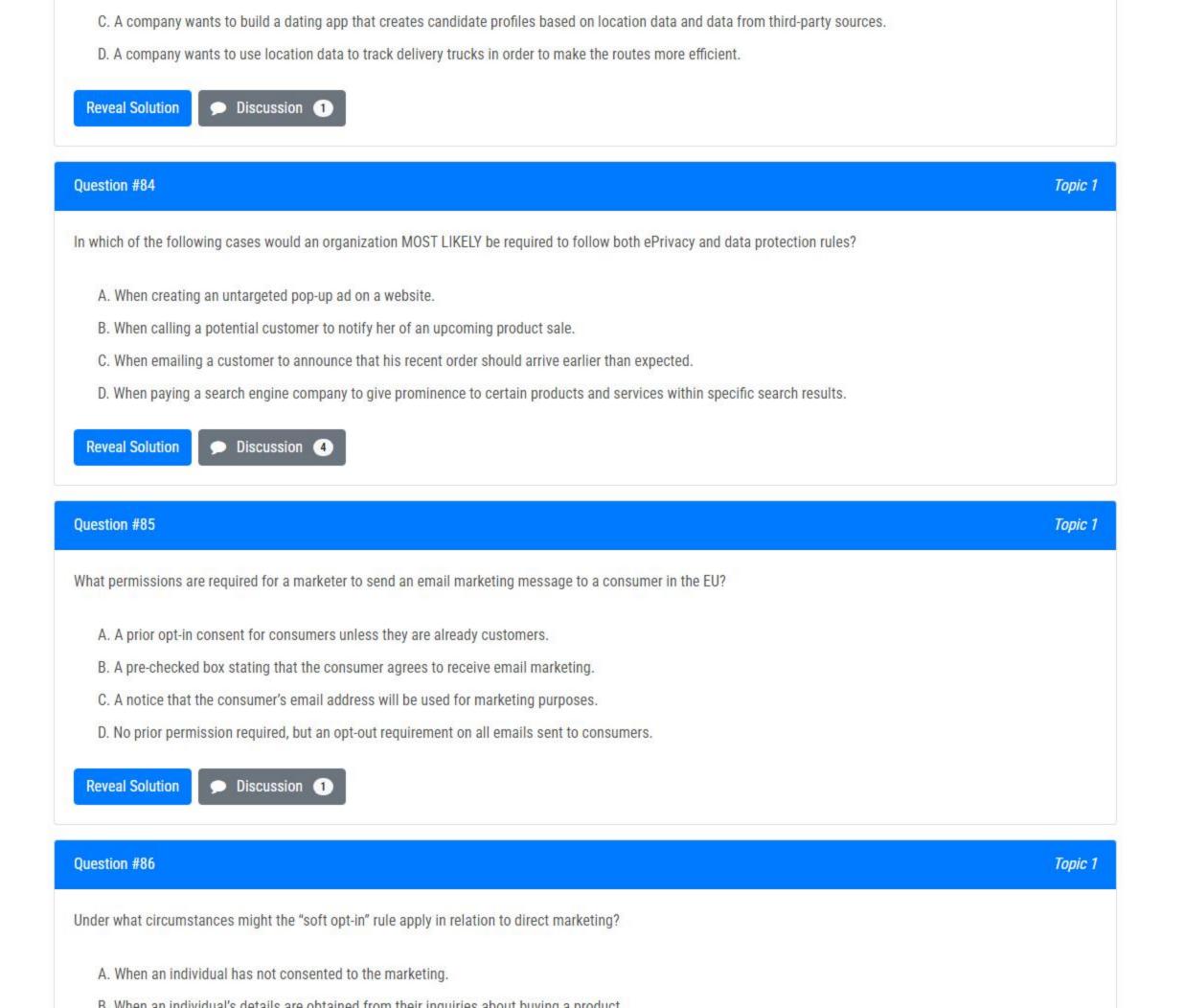
**Reveal Solution** 

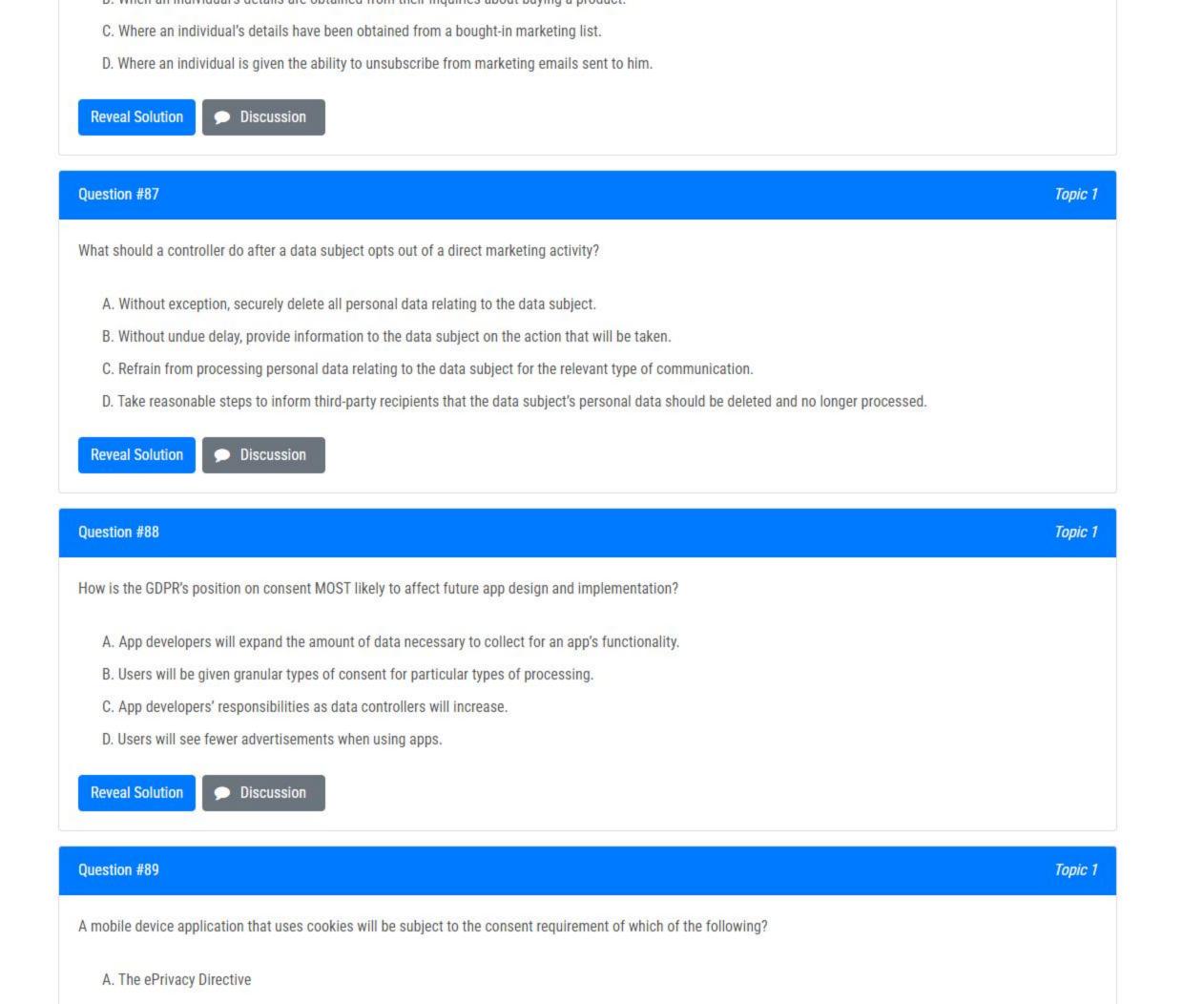


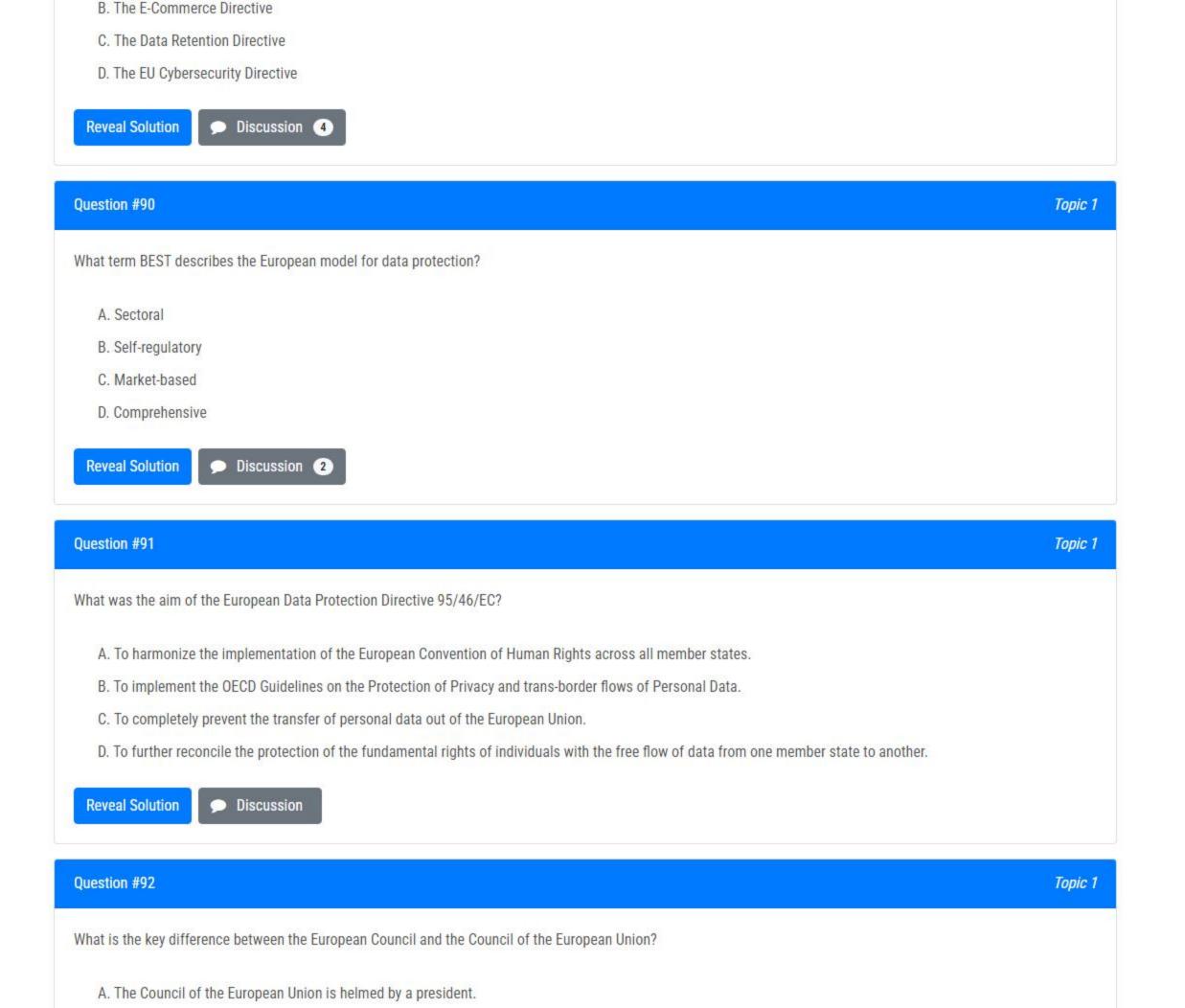
Question #83 Topic 1

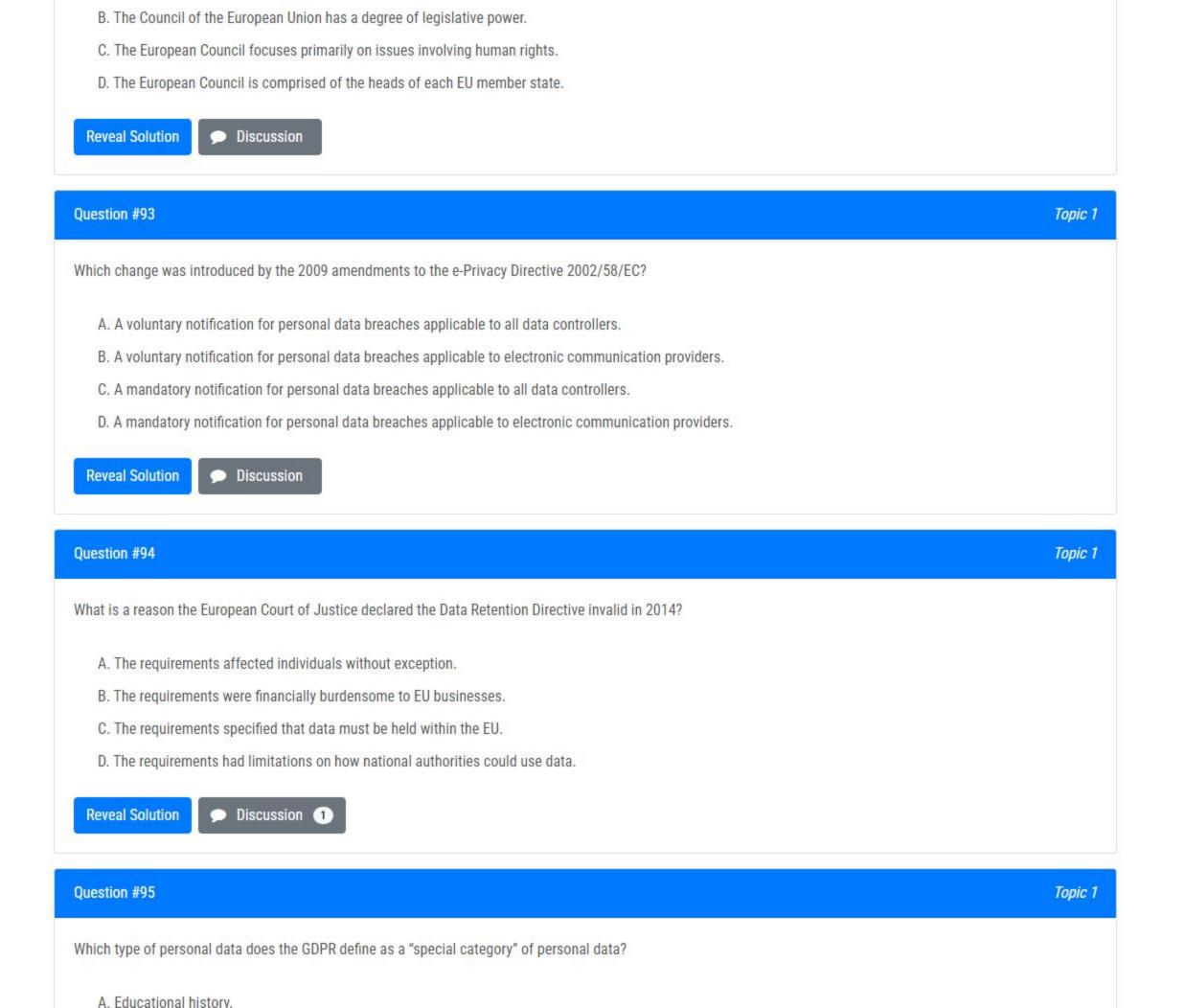
Based on GDPR Article 35, which of the following situations would trigger the need to complete a DPIA?

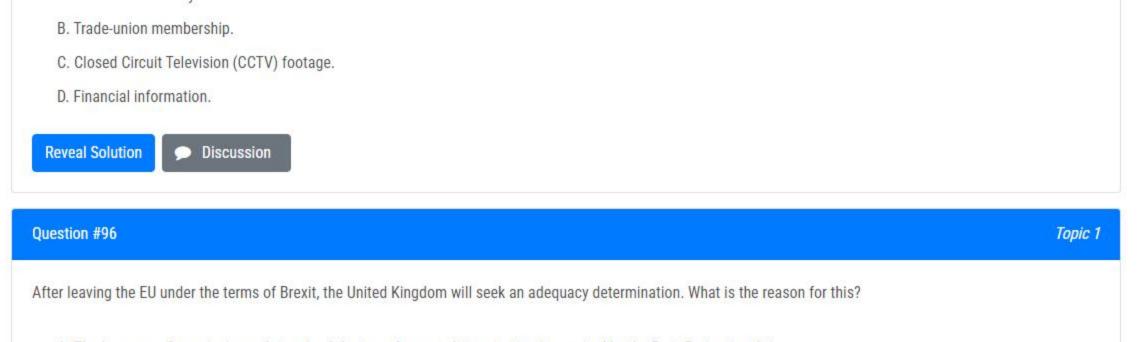
- A. A company wants to combine location data with other data in order to offer more personalized service for the customer.
- B. A company wants to use location data to infer information on a person's clothes purchasing habits.

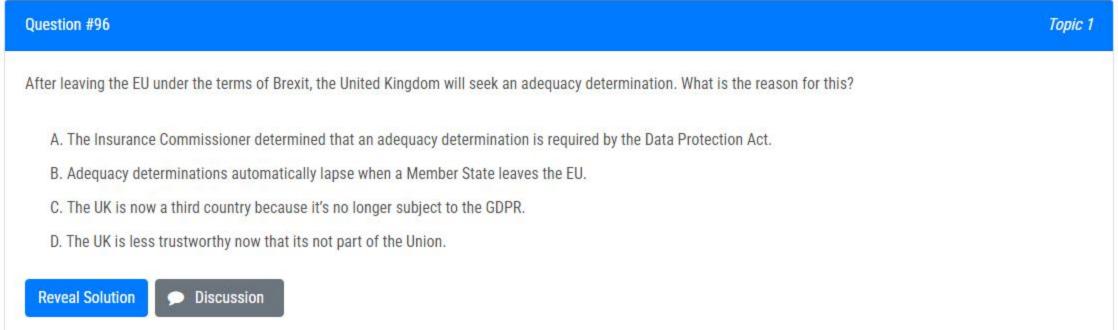


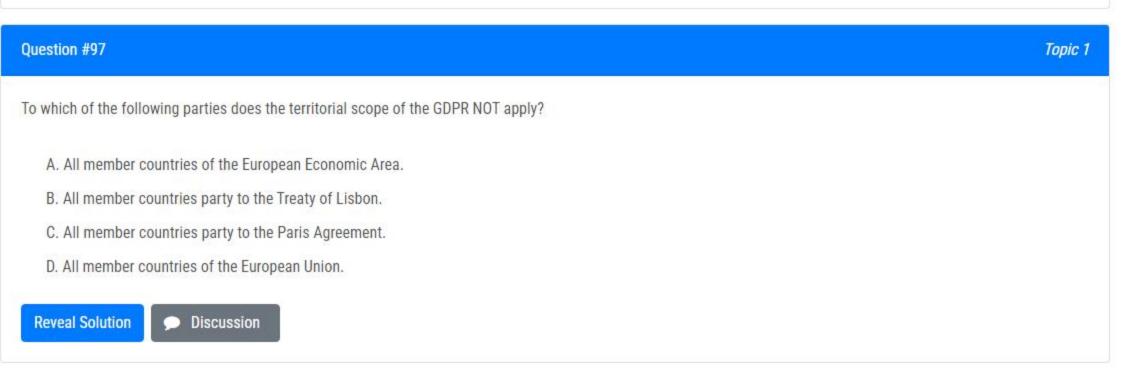


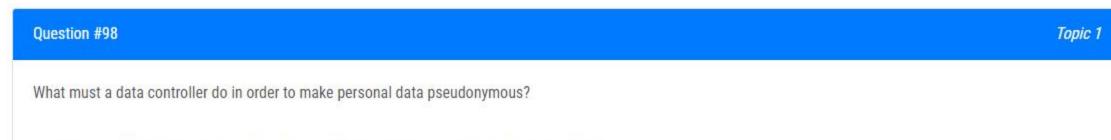


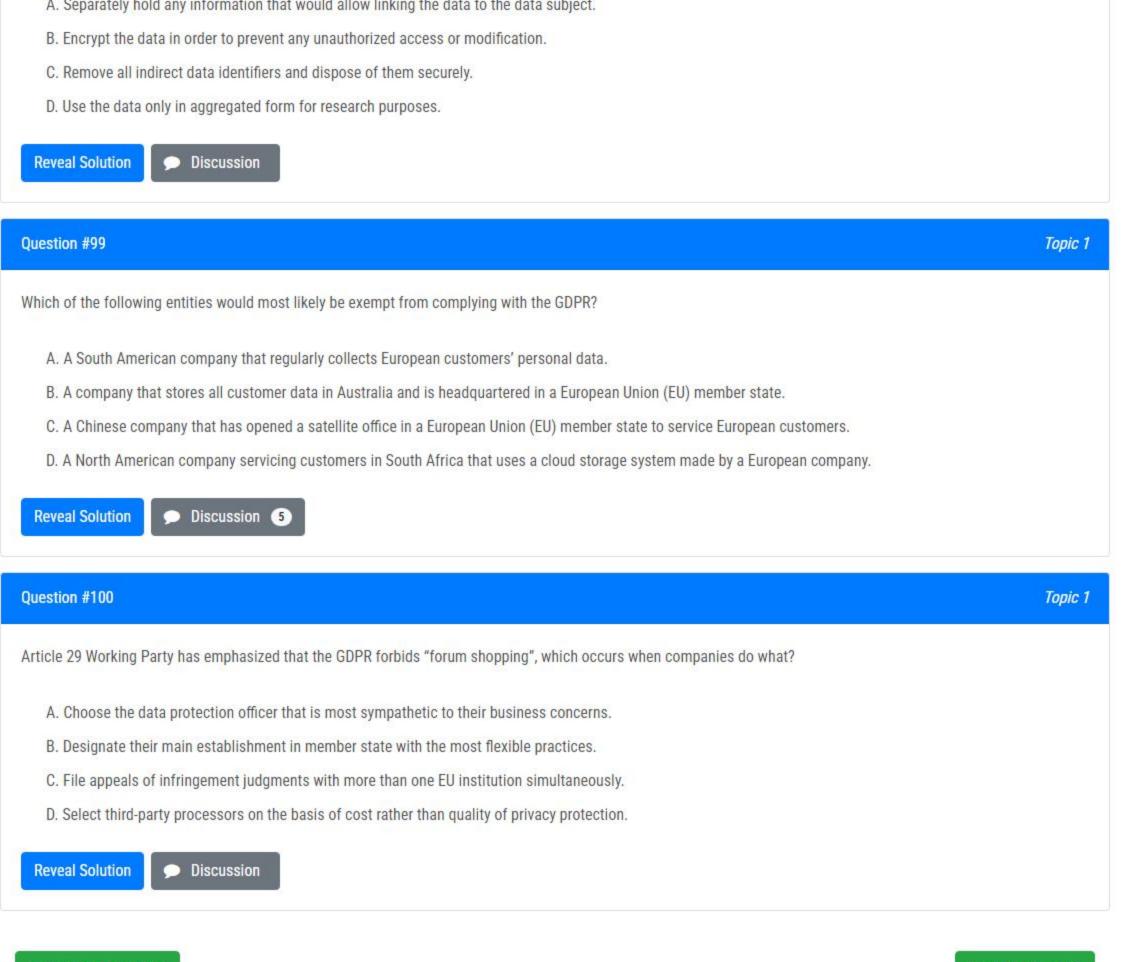




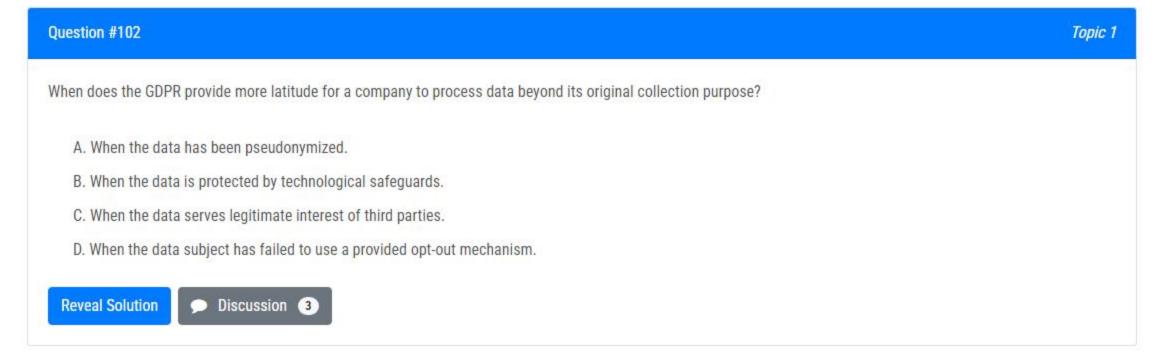










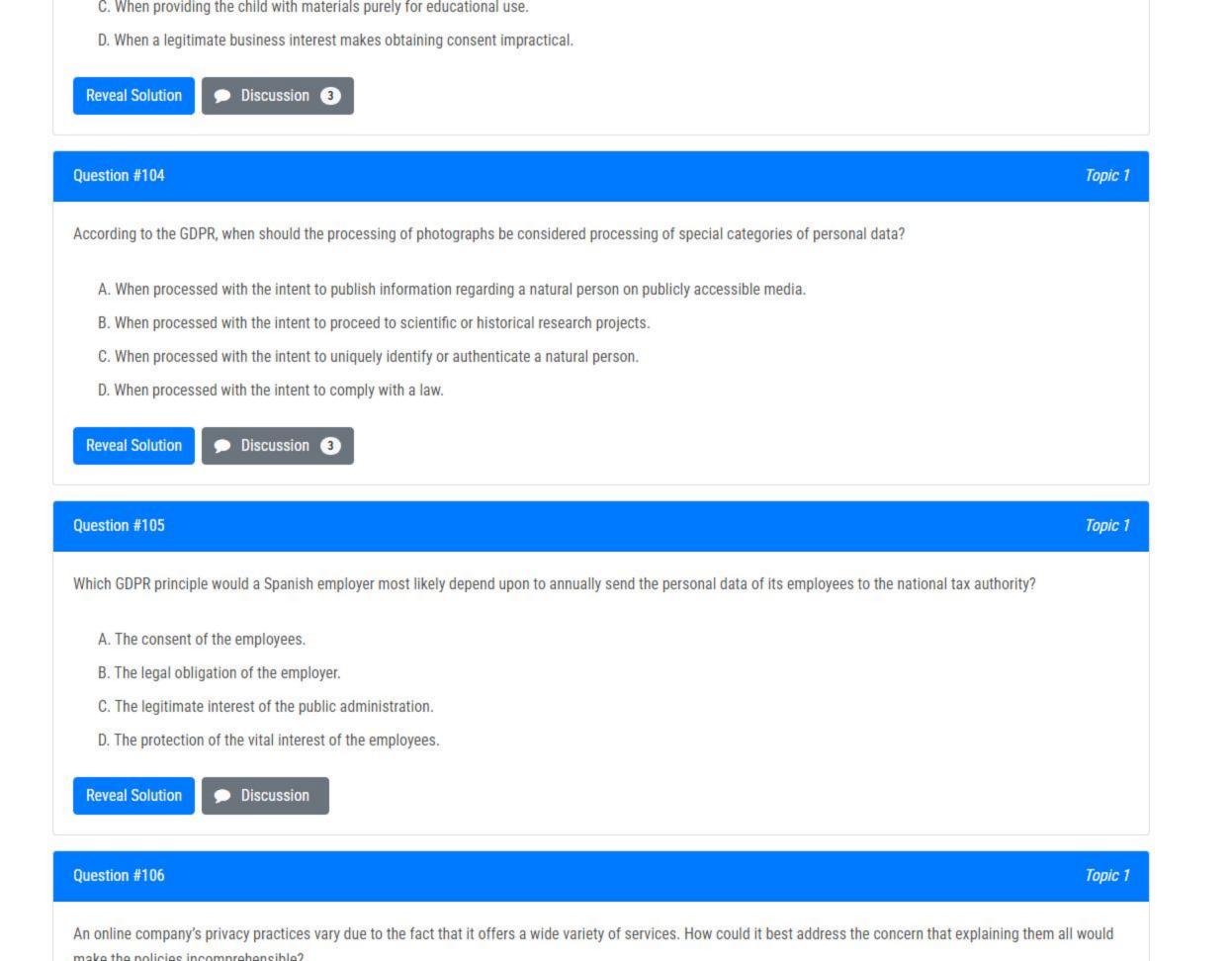


Question #103

In which situation would a data controller most likely be able to justify the processing of the data of a child without parental consent?

A. When the data is to be processed for market research.

B. When providing preventive or counselling services to the child.



A. Use a layered privacy notice on its website and in its email communications.

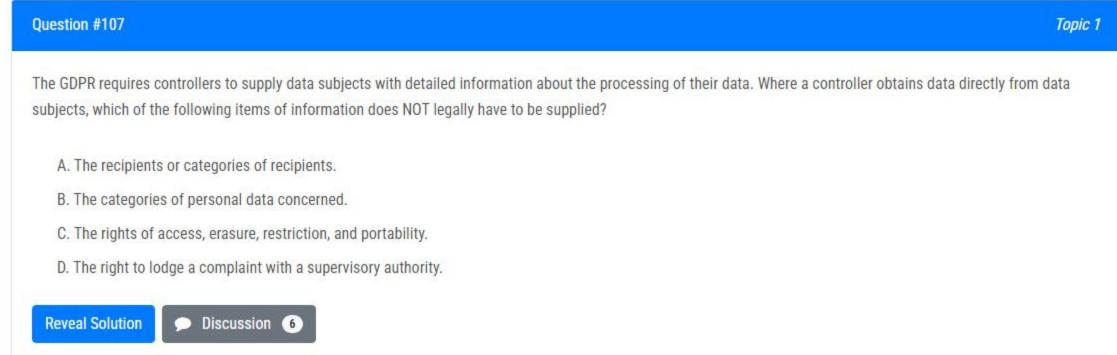
B. Identify uses of data in a privacy notice mailed to the data subject.

C. Provide only general information about its processing activities and offer a toll-free number for more information.

D. Place a banner on its website stipulating that visitors agree to its privacy policy and terms of use by visiting the site.

Reveal Solution

Discussion



According to Article 14 of the GDPR, how long does a controller have to provide a data subject with necessary privacy information, if that subject's personal data has been obtained from other sources?

A. As soon as possible after obtaining the personal data.

B. As soon as possible after the first communication with the data subject.

C. Within a reasonable period after obtaining the personal data, but no later than one month.

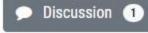
D. Within a reasonable period after obtaining the personal data, but no later than eight weeks.

Power Colution Discussion

D. When the processing is based on consent.

**Reveal Solution** 

Question #110



In which of the following situations would an individual most likely to be able to withdraw her consent for processing?

- A. When she is leaving her bank and moving to another bank.
- B. When she has recently changed jobs and no longer works for the same company.
- C. When she disagrees with a diagnosis her doctor has recorded on her records.
- D. When she no longer wishes to be sent marketing materials from an organization.

**Reveal Solution** 



Discussion

Question #111

Topic 1

Topic 1

As a result of the European Court of Justice's ruling in the case of Google v. Spain, search engines outside the EEA are also likely to be subject to the Regulation's right to be forgotten. This holds true if the activities of an EU subsidiary and its U.S. parent are what?

- A. Supervised by the same Data Protection Officer.
- B. Consistent with Privacy Shield requirements



**Reveal Solution** 

Discussion

Question #112 Topic 1

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

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

Reveal Solution

Discussion

Question #113 Topic 1

What are the obligations of a processor that engages a sub-processor?

- A. The processor must give the controller prior written notice and perform a preliminary audit of the sub-processor.
- B. The processor must obtain the controller's specific written authorization and provide annual reports on the sub-processor's performance.
- C. The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.
- D. The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.

Reveal Solution

Discussion

Question #114

What must be included in a written agreement between the controller and processor in relation to processing conducted on the controller's behalf?

- A. An obligation on the processor to report any personal data breach to the controller within 72 hours.
- B. An obligation on both parties to report any serious personal data breach to the supervisory authority.
- C. An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
- D. 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.

**Reveal Solution** 

Discussion

Question #115 Topic 1

To provide evidence of GDPR compliance, a company performs an internal audit. As a result, it finds a data base, password-protected, listing all the social network followers of the client.

Regarding the domain of the controller-processor relationships, how is this situation considered?

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

**Reveal Solution** 

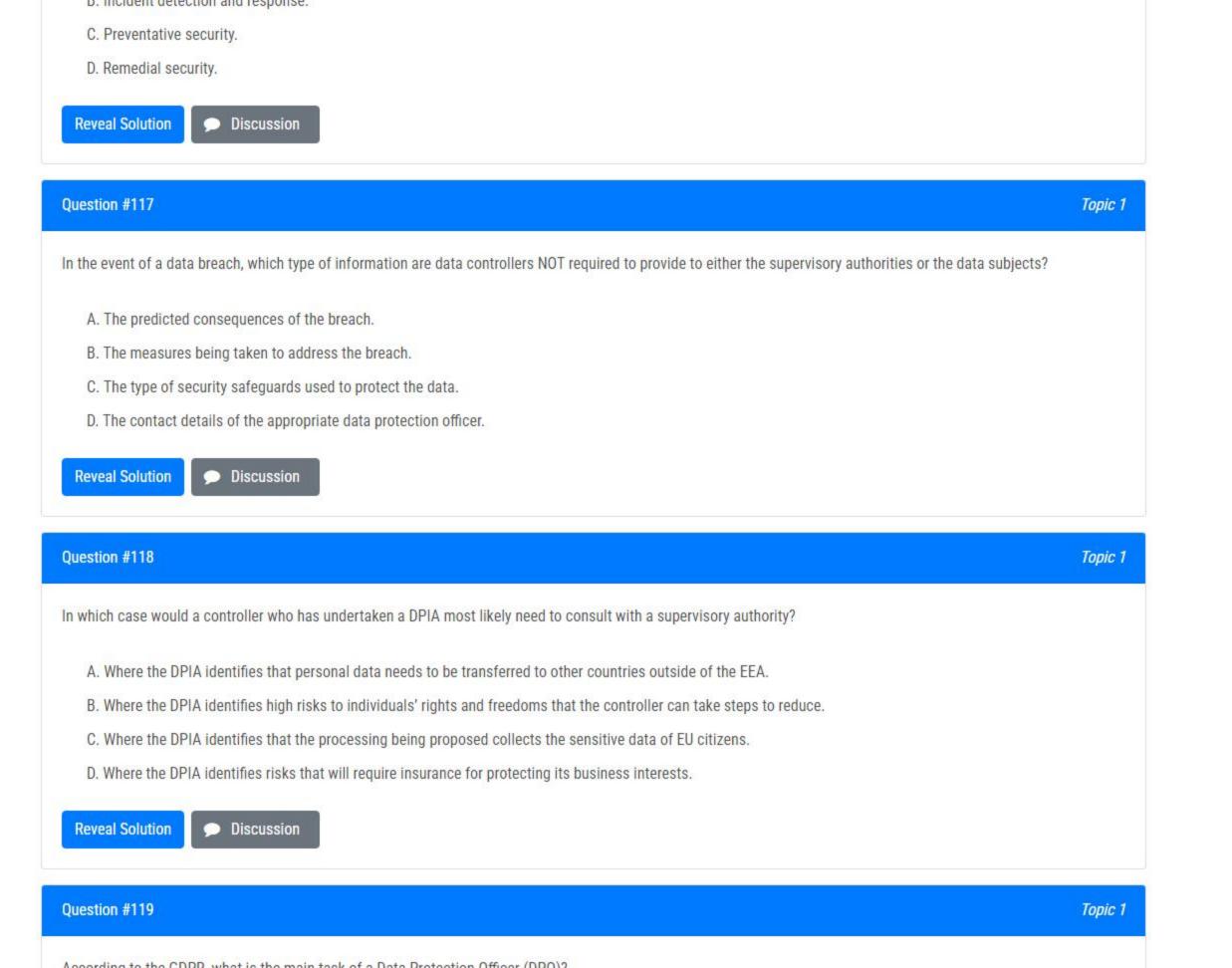
Discussion

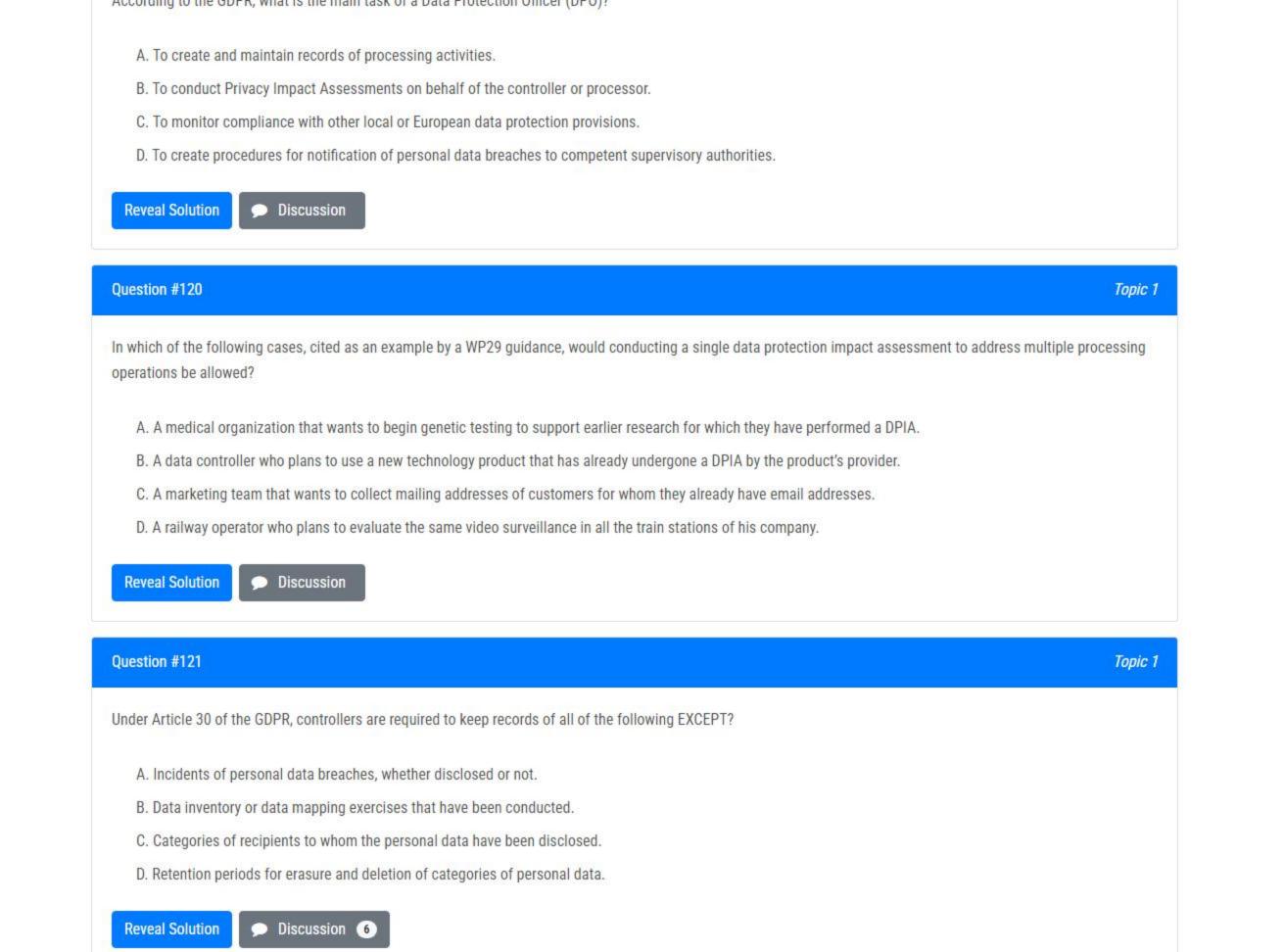
Question #116

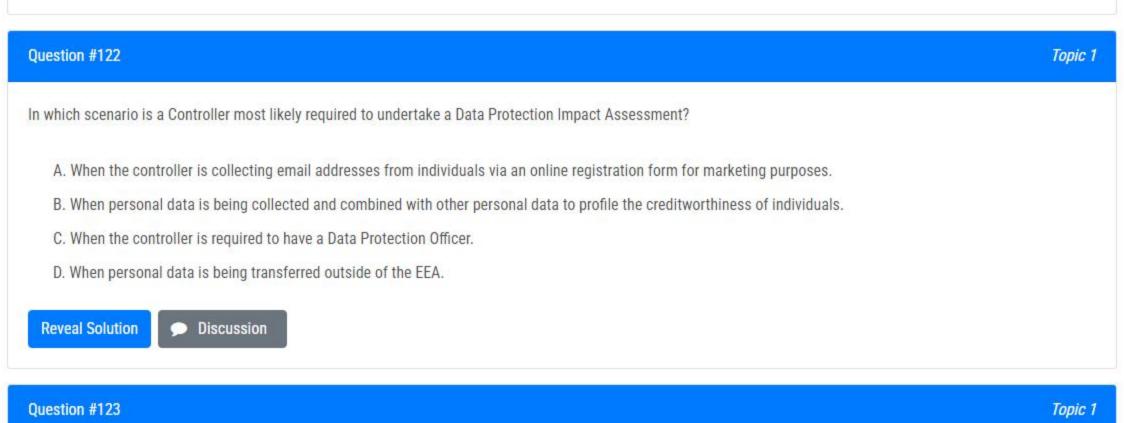
There are three domains of security covered by Article 32 of the GDPR that apply to both the controller and the processor. These include all of the following EXCEPT?

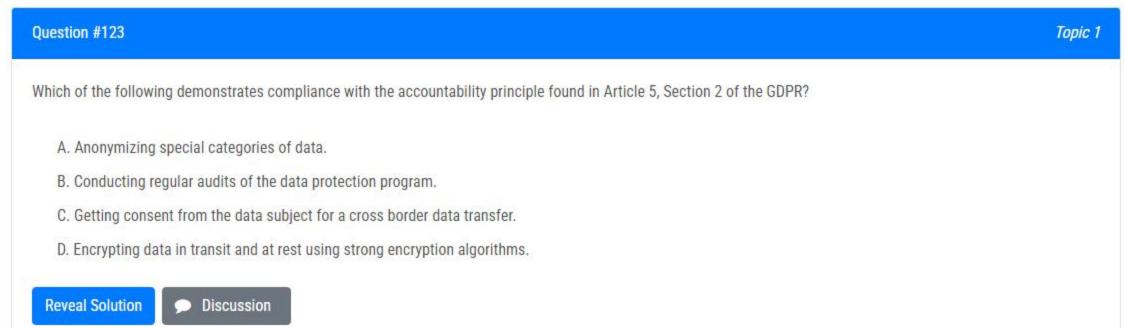
Topic 1

- A. Consent management and withdrawal.
- D. Incident detection and recognes









# Question #124 Topic 1

## SCENARIO -

Please use the following to answer the next question:

Dynaroux Fashion ('Dynaroux') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland.

Ronan is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.

The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of

information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.

In an aggressive bid to build revenue growth, Jonas, the CEO, tells Ronan that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Ronan tells the CEO that: (a) the potential risks of such activities means that Dynaroux needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures, Dynaroux may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.

Jonas tells Ronan that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Dynaroux's business plan and associated processing activities.

Which of the following facts about Dynaroux would trigger a data protection impact assessment under the GDPR?

- A. The company will be undertaking processing activities involving sensitive data categories such as financial and children's data.
- B. The company employs approximately 650 people and will therefore be carrying out extensive processing activities.
- C. The company plans to undertake profiling of its customers through analysis of their purchasing patterns.
- D. The company intends to shift their business model to rely more heavily on online shopping.

Reveal Solution Discussion

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

A. Approved certifications.

B. Binding corporate rules.

C. Law enforcement requests.

D. Standard contractual clauses.

Question #126 Topic 1

Which sentence best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

- A. Employees must sign an ad hoc contractual agreement each time personal data is exported.
- B. All employees are subject to the rules in their entirety, regardless of where the work is taking place.
- C. All employees must follow the privacy regulations of the jurisdictions where the current scope of their work is established.
- D. Employees who control personal data must complete a rigorous certification procedure, as they are exempt from legal enforcement.

Reveal Solution

Discussion

Question #127 Topic 1

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

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

**Reveal Solution** 

Discussion 2

Question #128 Topic 1

# 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?

- A. Germany, because that is where T-Craze is headquartered.
- B. France, because that is where T-Craze conducts processing of personal information.
- C. Spain, because that is T-Craze's primary market based on its marketing campaigns.
- D. T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.

Reveal Solution

Discussion 5

Question #129 Topic 1

# 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.

Why does the Spanish supervisory authority notify the French supervisory authority when it opens an investigation into T-Craze based on Sofia's complaint?

- A. T-Craze has a French affiliate.
- B. The French affiliate procured the services of Right Target.
- C. T-Craze conducts its marketing and sales activities in France.
- D. The Spanish supervisory authority is providing a courtesy notification not required under the GDPR.



Question #130 Topic 1

## 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.

What is the best option for the lead regulator when responding to the Spanish supervisory authority's notice that it plans to take action regarding Sofia's complaint?

- A. Accept, because it did not receive any complaints.
- B. Accept, because GDPR permits non-lead authorities to take action for such complaints.
- C. Reject, because Right Target's processing was conducted throughout Europe.
- D. Reject, because GDPR does not allow other supervisory authorities to take action if there is a lead authority.



Question #131 Topic 1

Which of the following is one of the supervisory authority's investigative powers?

- A. To notify the controller or the processor of an alleged infringement of the GDPR.
- B. To require that controllers or processors adopt approved data protection certification mechanisms.
- C. To determine whether a controller or processor has the right to a judicial remedy concerning a compensation decision made against them.
- D. To require data controllers to provide them with written notification of all new processing activities.



Question #132 Topic 1

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?

- A. Because use of biometric data to confirm the unique identification of data subjects benefits from an exemption.
- B. Because photographs qualify as biometric data only when they undergo a "specific technical processing".
- C. Because employees are deemed to have given their explicit consent when they agree to be photographed by their employer.
- D. Because photographic ID is a physical security measure which is "necessary for reasons of substantial public interest".

Reveal Solution Discussion 1

Question #133 Topic 1

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

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

Reveal Solution Discussion

Question #134 Topic 1

Which of the following is NOT a role of works councils?

- A. Determining the monetary fines to be levied against employers for data breach violations of employee data.
- B. Determining whether to approve or reject certain decisions of the employer that affect employees.
- C. Determining whether employees' personal data can be processed or not.
- D. Determining what changes will affect employee working conditions.

Reveal Solution Discussion 1

Question #135 Topic 1

Under the Data Protection Law Enforcement Directive of the EU, a government can carry out covert investigations involving personal data, as long it is set forth by law and constitutes a measure that is both necessary and what?

- A. Prudent.
- B. Important.
- C. Proportionate.
- D. DPA-approved.

Reveal Solution

Discussion

Question #136 Topic 1

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



- B. Processing of special categories of personal data on a large scale requires appointing a DPO.
- C. Personal data of data subjects must always be accurate and kept up to date.
- D. Data controllers must be in control of the data they hold at all times.

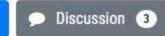


Question #137 Topic 1

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

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

**Reveal Solution** 

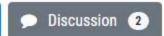


Question #138 Topic 1

Which of the following is an example of direct marketing that would be subject to European data protection laws?

- A. An updated privacy notice sent to an individual's personal email address.
- B. A charity fundraising event notice sent to an individual at her business address.
- C. A service outage notification provided to an individual by recorded telephone message.
- D. A revision of contract terms conveyed to an individual by SMS from a marketing organization.

Reveal Solution

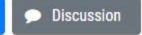


Question #139 Topic 1

Article 9 of the GDPR lists exceptions to the general prohibition against processing biometric data. Which of the following is NOT one of these exceptions?

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

**Reveal Solution** 



Question #140 Topic 1

Which marketing-related activity is least likely to be covered by the provisions of Privacy and Electronic Communications Regulations (Directive 2002/58/EC)?

- A. Advertisements passively displayed on a website.
- B. The use of cookies to collect data about an individual.
- C. A text message to individuals from a company offering concert tickets for sale.
- D. An email from a retail outlet promoting a sale to one of their previous customer.



Question #141 Topic 1

Which of the following is NOT recognized as being a common characteristic of cloud-computing services?

- A. The service's infrastructure is shared among the supplier's customers and can be located in a number of countries.
- B. The supplier determines the location, security measures, and service standards applicable to the processing.
- C. The supplier allows customer data to be transferred around the infrastructure according to capacity.
- D. The supplier assumes the vendor's business risk associated with data processed by the supplier.

Reveal Solution Discussion

Question #142 Topic 1

When may browser settings be relied upon for the lawful application of cookies?

- A. When a user rejects cookies that are strictly necessary.
- B. When users are aware of the ability to adjust their settings.
- C. When users are provided with information about which cookies have been set.
- D. When it is impossible to bypass the choices made by users in their browser settings.

Reveal Solution Discussion 2

Question #143 Topic 1

# SCENARIO -

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

# Registration Form -

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)

Vigotron values your privacy. The M-Health app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)

Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third-party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

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

First name:

Surname:

Year of birth:

Email:

Physical Address (optional\*):

Health status:

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

Terms and Conditions 
1. Jurisdiction. [...]

2. Applicable law. [...]

3. Limitation of liability. [...]

# Consent -

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

Emily sends the draft to Sam for review. Which of the following is Sam most likely to point out as the biggest problem with Emily's consent provision?

- A. It is not legal to include fields requiring information regarding health status without consent.
- B. Processing health data requires explicit consent, but the form does not ask for explicit consent.
- C. Direct marketing requires explicit consent, whereas the registration form only provides for a right to object
- D. The provision of the fitness app should be made conditional on the consent to the data processing for direct marketing.



Question #144 Topic 1

# SCENARIO -

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

# Registration Form -

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)

Vigotron values your privacy. The M-Health app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)

Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third-party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

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

First name:

Surname:

Year of birth:

Email:

Physical Address (optional\*):

Health status:

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

Terms and Conditions -

- 1. Jurisdiction, [...]
- 2. Applicable law. [...]
- 3. Limitation of liability. [...]

# Consent -

By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any

required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.

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

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



Question #145 Topic 1

# SCENARIO -

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

#### Registration Form -

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.)

Vigotron values your privacy. The M-Health app allows you to decide which information is stored in it, and which apps can access your data. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.)

Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third-party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

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

First name:

Surname:

Year of birth:

Email:

Physical Address (optional\*):

Health status:

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

Terms and Conditions

- 1. Jurisdiction. [...]
- 2. Applicable law. [...]
- 3. Limitation of liability. [...]

# Consent -

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

What is one potential problem Vigotron's age policy might encounter under the GDPR?

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



Question #146 Topic 1

## 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.

Based on the GDPR's position on the use of personal data for direct marketing purposes, which of the following is true about Louis's rights as a data subject?

- A. Louis does not have the right to object to the use of his data because he previously consented to it.
- B. Louis has the right to object at any time to the use of his data and Bedrock must honor his request to cease use.
- C. Louis has the right to object to the use of his data, unless his data is required by Bedrock for the purpose of exercising a legal claim.
- D. Louis does not have the right to object to the use of his data if Bedrock can demonstrate compelling legitimate grounds for the processing.



Question #147 Topic 1

# SCENARIO -

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third-party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated

Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.

Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box's home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box's Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.

Despite some customer complaints, Brady's business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad

network with whom he has set clearly defined roles. Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and services.

Based on the scenario, what is the main reason that Brady should be concerned with Hermes Designs' handling of customer personal data?

- A. The data is sensitive.
- B. The data is uncategorized.
- C. The data is being used for a new purpose.
- D. The data is being processed via a new means.



Question #148 Topic 1

# SCENARIO -

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third-party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated

Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.

Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box's home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box's Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.

Despite some customer complaints, Brady's business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad network with whom he has set clearly defined roles. Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and services.

Based on current trends in European privacy practices, which aspect of Brady Box' Online Behavioral Advertising (OBA) is most likely to be insufficient if the company becomes established in Europe?

- A. The lack of the option to opt in.
- B. The level of security within the website.
- C. The contract with the third-party advertising network.
- D. The need to have the contents of the advertising approved.

Reveal Solution Discussion 2

Question #149 Topic 1

# SCENARIO -

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third-party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his

customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated

Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.

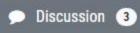
Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box's home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box's Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.

Despite some customer complaints, Brady's business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad network with whom he has set clearly defined roles. Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and services.

Under the General Data Protection Regulation (GDPR), what is the most likely reason Serge may have grounds to object to the use of his quotation?

- A. Because of the misrepresentation of personal data as an endorsement.
- B. Because of the juxtaposition of the quotation with others' quotations.
- C. Because of the use of personal data outside of the social networking service (SNS).
- D. Because of the misapplication of the household exception in relation to a social networking service (SNS).

Reveal Solution



Question #150 Topic 1

# SCENARIO -

Please use the following to answer the next question:

TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.

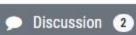
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories – age, income, ethnicity – that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.

Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.

After Leon has informed his manager, what is Techiva's legal responsibility as a processor?

- A. They must report it to TripBliss Inc.
- B. They must conduct a full systems audit.
- C. They must report it to the supervisory authority.
- D. They must inform customers who have used the website.

**Reveal Solution** 



Question #151 Topic 1

# 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 Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information. If Who-R-U decides to track locations using its app, what must it do to comply with the GDPR?

- A. Get consent from the app users.
- B. Provide a transparent notice to users.
- C. Anonymize the data and add latency so it avoids disclosing real time locations.
- D. Obtain a court order because location data is a special category of personal data.



Question #152 Topic 1

# 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 Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information. The Customer for Life plan may conflict with which GDPR provision?

- A. Article 6, which requires processing to be lawful.
- B. Article 7, which requires consent to be as easy to withdraw as it is to give

and market and and and and an artist of the second of the second and an artist of the second and a second and The second of the second and are second as the second of the second and are second as the second and are second

C. Article 16, which provides data subjects with a rights to rectification.

D. Article 20, which gives data subjects a right to data portability.

Reveal Solution Discussion

Question #153 Topic 1

#### 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 Canada. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information. If Who-R-U adopts the We-Track-U pilot plan, why is it likely to be subject to the territorial scope of the GDPR?

- A. Its plan would be in the context of the establishment of a controller in the Union.
- B. It would be offering goods or services to data subjects in the Union.
- C. It is engaging in commercial activities conducted in the Union.
- D. It is monitoring the behavior of data subjects in the Union.

Reveal Solution



Question #154 Topic 1

# 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 Canada. 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?

A. The company isn't a controller established in the Union.

B. The laptop belonged to a company located in Canada.

C. The data isn't considered personally identifiable financial information.

D. There is no evidence that the thieves have accessed the data on the laptop.

Reveal Solution

Discussion

Discussion

Question #155 Topic 1

## 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 data. 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?

- A. How often promotional emails will be sent.
- B. Contact information of the hosting company.
- C. Technical and organizational measures to protect data.
- D. The categories of recipients with whom data will be shared.

Reveal Solution Discussion 1

Question #156 Topic 1

# 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 data. 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 must the contract between WonderKids and the hosting service provider contain?



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 data. 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 direct marketing information can WonderKids send by email without prior consent of the person booking the childcare?

- A. No marketing information at all.
- B. Any marketing information at all.
- C. Marketing information related to other business operations of WonderKids.
- D. Marketing information for products or services similar to those purchased from WonderKids.



#### Question #158 Topic 1

An organization conducts body temperature checks as a part of COVID-19 monitoring. Body temperature is measured manually and is not followed by registration, documentation or other processing of an individual's personal data.

Which of the following best explain why this practice would NOT be subject to the GDPR?

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



Question #159 Topic 1

When assessing the level of risk created by a data breach, which of the following would NOT have to be taken into consideration?

- A. The ease of identification of individuals.
- B. The size of any data processor involved



D. The nature, sensitivity and volume of personal data.

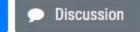


Question #160 Topic 1

Under Article 80(1) of the GDPR, individuals can elect to be represented by not-for-profit organizations in a privacy group litigation or class action. These organizations are commonly known as?

- A. Law firm organizations.
- B. Civil society organizations.
- C. Human rights organizations.
- D. Constitutional rights organizations.

**Reveal Solution** 



Question #161 Topic 1

# SCENARIO -

Please use the following to answer the next question:

BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information – name, location, and prior purchase history – with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens. Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.

What is the nature of BHealthy and Natural Insight's relationship?

- A. Natural Insight is BHealthy's processor because the companies entered into data processing terms.
- B. Natural Insight is BHealthy's processor because BHealthy is sharing its customer information with Natural Insight.
- C. Natural Insight is the controller because it determines the security measures to implement to protect data it processes; BHealthy is a co-controller because it engaged Natural Insight to determine pricing for the new sunscreens.
- D. Natural Insight is a controller because it is separately determining the purpose of processing when it uses BHealthy's customer information to improve its machine learning algorithms.

Reveal Solution



Question #162 Topic 1

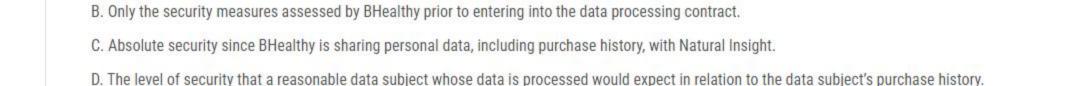
# SCENARIO -

Please use the following to answer the next question:

BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information – name, location, and prior purchase history – with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens. Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.

Under the GDPR, what are Natural Insight's security obligations with respect to the customer information it received from BHealthy?

A. Appropriate security that takes into account the industry practices for protecting customer contact information and purchase history.



Topic 1

### SCENARIO -

Question #163

**Reveal Solution** 

Please use the following to answer the next question:

Discussion

BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information – name, location, and prior purchase history – with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens. Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.

In which case would Natural Insight's use of BHealthy's data for improvement of its algorithms be considered data processor activity?

- A. If Natural Insight uses BHealthy's data for improving price point predictions only for BHealthy.
- B. If Natural Insight receives express contractual instructions from BHealthy to use its data for improving its algorithms.
- C. If Natural Insight agrees to be fully liable for its use of BHealthy's customer information in its product improvement activities.
- D. If Natural Insight satisfies the transparency requirement by notifying BHealthy's customers of its plans to use their information for its product improvement activities.

Reveal Solution Discussion

Question #164 Topic 1

Which of the following is NOT an explicit right granted to data subjects under the GDPR?

- A. The right to request access to the personal data a controller holds about them.
- B. The right to request the deletion of data a controller holds about them.
- C. The right to opt-out of the sale of their personal data to third parties.
- D. The right to request restriction of processing of personal data, under certain scenarios.

Reveal Solution Discussion

Question #165 Topic 1

As per the GDPR, which legal basis would be the most appropriate for an online shop that wishes to process personal data for the purpose of fraud prevention?

- A. Protection of the interests of the data subjects.
- B. Performance of a contact
- C. Legitimate interest
- D. Consent

Reveal Solution Discussion

Question #166 Topic 1

The Planet 49 CJEU Judgement applies to?

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

Reveal Solution Discussion

Question #167 Topic 1

Bioface is a company based in the United States. It has no servers, personnel or assets in the European Union. By collecting photographs from social media and other web-based services, such as newspapers and blogs, it uses machine learning to develop a facial recognition algorithm. The algorithm identifies individuals in photographs who are not in its data set based the algorithm and its existing data. The service collects photographs of data subjects in the European Union and will identify them if presented with their photographs. Bioface offers its service to government agencies and companies in the United States and Canada, but not to those in the European Union. Bioface does not offer the service to individuals.

Why is Bioface subject to the territorial scope of the General Data Protection Regulation?

- A. It collects data from European Union websites, which constitutes an establishment in the European Union.
- B. It offers services in the European Union by identifying data subjects in the European Union.
- C. It collects data from subjects and uses it for automated processing.
- D. It monitors the behavior of data subjects in the European Union.

Reveal Solution Discussion 3

Question #168 Topic 1

# 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.

When Ben had the company collect additional data from its customers, the most serious violation of the GDPR occurred because the processing of the data created what?

- A. An information security risk by copying the data into a new database.
- B. A potential legal liability and financial exposure from its customers.
- C. A significant risk to the customers' fundamental rights and freedoms.
- D. A significant risk due to the lack of an informed consent mechanism.

Reveal Solution Discussion

Question #169 Topic 1

#### 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?

- A. Send out consent forms to all of its employees.
- B. Minimize the amount of data collected for the lawsuit.
- C. Inform all of its employees about the lawsuit.
- D. Encrypt the data from all of its employees.



Question #170 Topic 1

# 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.

As a result of Sam's actions, the Gummy Bear Company potentially violated Articles 33 and 34 of the GDPR and will be required to do what?



- B. Analyze and evaluate the liability for customers in Ireland.
- C. Analyze and evaluate all of its breach notification obligations.
- D. Notify all of its customers that reside in the European Union.



Question #171 Topic 1

#### 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.

The data transfer mechanism that Alice drafted violates the GDPR because the company did not first get approval from?

- A. The Court of Justice of the European Union.
- B. The European Data Protection Board.
- C. The Data Protection Authority.
- D. The European Commission.

Reveal Solution Discussion 4

Question #172 Topic 1

# SCENARIO -

Please use the following to answer the next question:

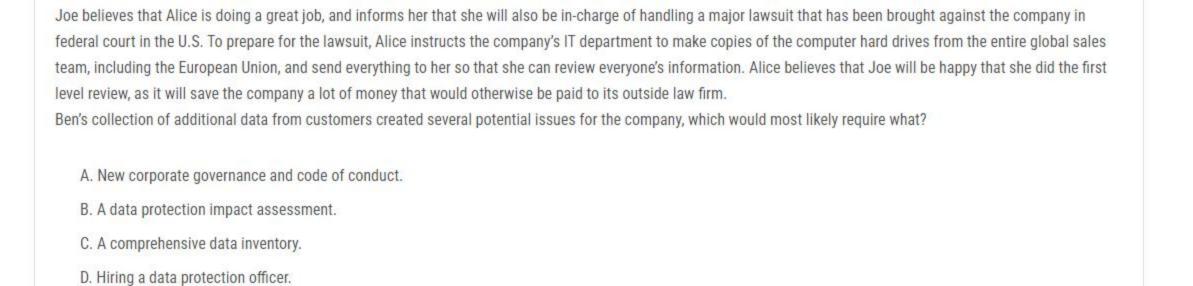
Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA. Today, it is a multi-billion-dollar candy company operating in every continent. All of the company's IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major 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.





Question #173

Which of the following was the first legally binding international instrument in the area of data protection?

A. Convention 108.

B. General Data Protection Regulation.

C. Universal Declaration of Human Rights.

D. EU Directive on Privacy and Electronic Communications.

Reveal Solution

Discussion

Question #174 Topic 1

A multinational company is appointing a mandatory data protection officer. In addition to considering the rules set out in Article 37 (1) of the GDPR, which of the following actions must the company also undertake to ensure compliance in all EU jurisdictions in which it operates?

- A. Consult national derogations to evaluate if there are additional cases to be considered in relation to the matter.
- B. Conduct a Data Protection Privacy Assessment on the processing operations of the company in all the countries it operates.
- C. Assess whether the company has more than 250 employees in each of the EU member-states in which it is established.
- D. Revise the data processing activities of the company that affect more than one jurisdiction to evaluate whether they comply with the principles of privacy by design and by default.

Reveal Solution Discussion

Question #175 Topic 1

The European Parliament jointly exercises legislative and budgetary functions with which of the following?

- A. The European Commission.
- B. The Article 29 Working Party.
- C. The Council of the European Union.
- D. The European Data Protection Board.

Reveal Solution Discussion 3

A U.S. company's website sells widgets. Which of the following factors would NOT in itself subject the company to the GDPR?

A. The widgets are offered in EU and priced in euro.

B. The website is in English and French, and is accessible in France.

C. An affiliate office is located in France but the processing is in the U.S.

D. The website places cookies to monitor the EU website user behavior.

# When does the European Data Protection Board (EDPB) recommend reevaluating whether a transfer tool is effectively providing a level of personal data protection that is in compliance with the European Union (EU) level? A. After a personal data breach.

- B. Every three (3) years.
- C. On an ongoing basis.
- D. Every year.

Reveal Solution



Question #178 Topic 1

Which judicial body makes decisions on actions taken by individuals wishing to enforce their rights under EU law?

- A. Court of Auditors
- B. Court of Justice of European Union
- C. European Court of Human Rights
- D. European Data Protection Board

Question #179 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Discussion

Sandy recently joined Market 4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market4U maintains a list of 19 million global contacts that were collected throughout the course of Market4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.

Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market 4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.

What should Sandy give as feedback to Dan and the marketing team regarding the new fields Dan wants to add to Market4U's forms?

- A. Make all the fields optional.
- B. Only request the information in brackets (i.e., age group and salary range).
- C. Eliminate the fields, as they are not proportional to the services being offered.
- D. Eliminate the fields as they are not necessary for the purposes of providing white papers or registration for events.

Reveal Solution



Discussion 1

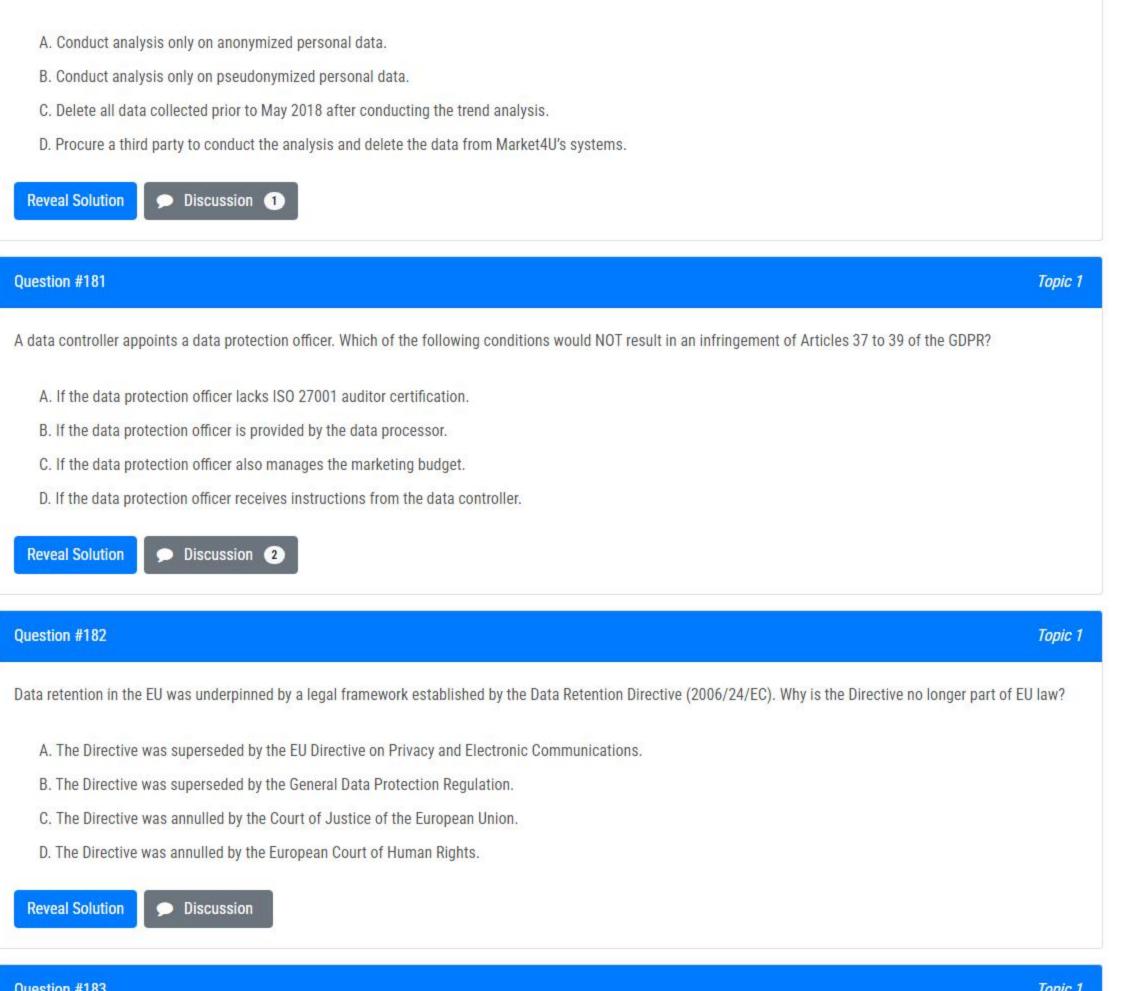
Question #180 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

Sandy recently joined Market 4U, an advertising technology company founded in 2016, as their VP of Privacy and Data Governance. Through her first initiative in conducting a data inventory, Sandy learned that Market 4U maintains a list of 19 million global contacts that were collected throughout the course of Market 4U's existence. Knowing the risk of having such a large amount of data, Sandy wanted to purge all contacts that were entered into Market4U's systems prior to May 2018, unless such contacts had a more recent interaction with Market4U content. However, Dan, the VP of Sales, informed Sandy that all of the contacts provide useful information regarding successful marketing campaigns and trends in industry verticals for Market4U's clients.

Dan also informed Sandy that he had wanted to focus on gaining more customers within the sports and entertainment industry. To assist with this behavior, Market 4U's marketing team decided to add several new fields to Market4U's website forms, including forms for downloading white papers, creating accounts to participate in Market4U's forum, and attending events. Such fields include birth date and salary.

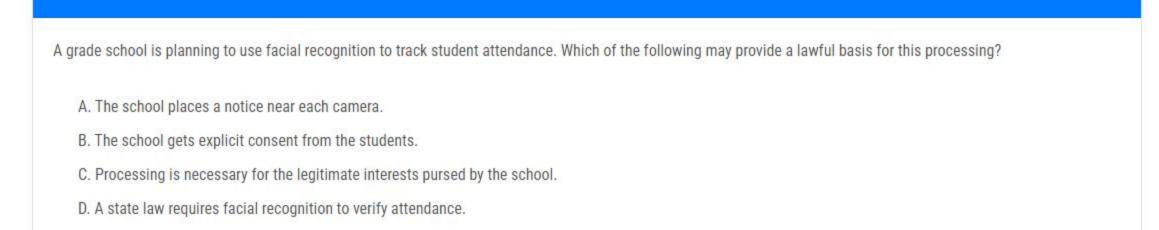


What is the best way that Sandy can gain the insights that Dan seeks while still minimizing risks for Market4U?

Question #183 Topic 1 Which of the following is the weakest lawful basis for processing employee personal data? A. Processing based on fulfilling an employment contract. B. Processing based on employee consent. C. Processing based on legitimate interests. D. Processing based on legal obligation. **Reveal Solution** Discussion Question #184 Topic 1 An organization receives a request multiple times from a data subject seeking to exercise his rights with respect to his own personal data. Under what condition can the organization charge the data subject a fee for processing the request? A. Only where the organization can show that it is reasonable to do so because more than one request was made. B. Only to the extent this is allowed under the restrictions on data subjects' rights introduced under Art 23 of GDPR. C. Only where the administrative costs of taking the action requested exceeds a certain threshold. D. Only if the organization can demonstrate that the request is clearly excessive or misguided. **Reveal Solution** Discussion Topic 1 Question #185 To receive a preliminary interpretation on provisions of the GDPR, a national court will refer its case to which of the following? A. The Court of Justice of the European Union. B. The European Data Protection Supervisor.

C. The European Court of Human Rights. D. The European Data Protection Board. Discussion **Reveal Solution** 

Question #186 Topic 1



Reveal Solution Discussion 3

Question #187 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.

Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain's locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.

Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.

What is the time period in which Mike should receive a response to his request?

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

Reveal Solution Discussion 2

Question #188 Topic 1

#### 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?

- A. ABC Hotel Chain is the controller and XYZ Travel Agency is the processor.
- B. XYZ Travel Agency is the controller and ABC Hotel Chain is the processor.
- C. ABC Hotel Chain and XYZ Travel Agency are independent controllers.
- D. ABC Hotel Chain and XYZ Travel Agency are joint controllers.

**Reveal Solution** 



Question #189 Topic 1

#### SCENARIO -

Please use the following to answer the next question:

10.14

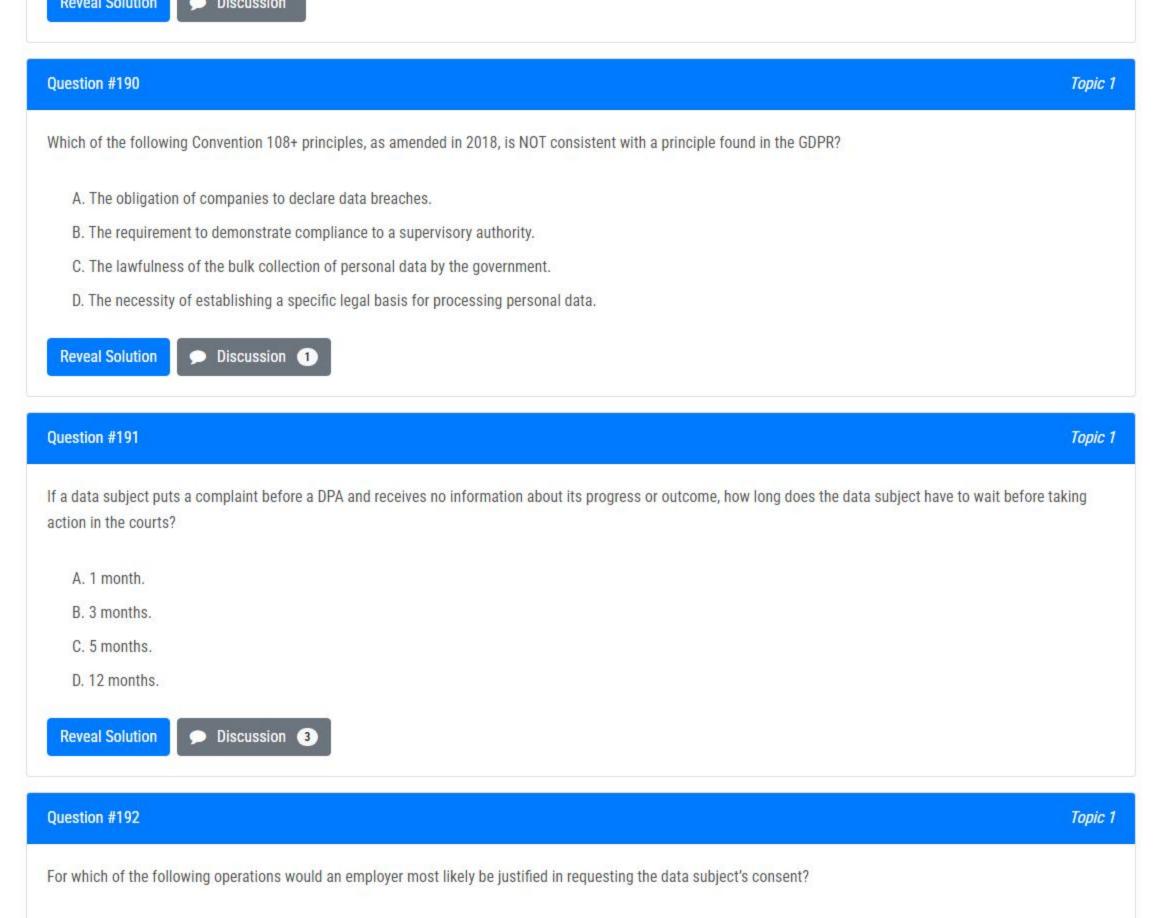
ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.

Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain's locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.

Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.

In which of the following situations would ABC Hotel Chain and XYZ Travel Agency NOT have to honor Mike's data access request?

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





C. Operating a CCTV system on company premises.

D. Assessing a potential employee's job application.

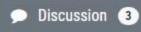


Question #193 Topic 1

An entity's website stores text files on EU users' computer and mobile device browsers. Prior to doing so, the entity is required to provide users with notices containing information and consent under which of the following frameworks?

- A. General Data Protection Regulation 2016/679.
- B. E-Privacy Directive 2002/58/EC.
- C. E-Commerce Directive 2000/31/EC.
- D. Data Protection Directive 95/46/EC.

**Reveal Solution** 



Question #194 Topic 1

Which of the following is NOT considered a fair processing practice in relation to the transparency principle?

- A. Providing a multi-layered privacy notice, in a website environment.
- B. Providing a QR code linking to more detailed privacy notice, in a CCTV sign.
- C. Providing a hyperlink to the organization's home page, in a hard copy application form.
- D. Providing a "just-in-time" contextual pop-up privacy notice, in an online application from field.

Reveal Solution



Question #195 Topic 1

Which of the following was the first to implement national law for data protection in 1973?

- A. France
- B. Sweden
- C. Germany

