Free Questions for CIPP-E

Shared by Stewart on 03-03-2025

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Start-up company MagicAI is developing an AI system that will be part of a medical device that detects skin cancer. To take measures against potential bias in its AI system, the IT team decides to collect data about users' ethnic origin, nationality, and gender. Which would be the most appropriate legal basis for this processing under GDPR, Article 9 (Processing of special categories of personal data)?

A. Processing necessary for scientific or statistical purposes. B. Processing necessary for reasons of substantial public interest. C. Processing necessary for purposes of preventive or occupational medicine. D. Processing necessary for the defense of legal claims in potential negligence cases.

Options:

Answer:

Explanation:

Under Article 9 of the GDPR, processing of special category data (e.g., ethnicity, health data) is prohibited unless an exception applies.

Why is C the correct answer?

AI-based medical devices fall under 'preventive or occupational medicine' as per GDPR Article 9(2)(h).

The AI system is used to detect skin cancer, a form of preventive medicine, making this the appropriate basis.

Why are other answers incorrect?

A (Scientific research or statistical purposes) While scientific research can be a legal basis, it requires additional safeguards such as anonymization, which may not be feasible in this case.

B (Substantial public interest) While public health is important, this processing is specific to medical diagnosis, making Article 9(2)(h) more appropriate.

D (Defense of legal claims) Legal claims are not relevant here, as the processing is for bias mitigation in AI training.

Question 2

Question Type: MultipleChoice

What monitoring may lawfully be performed within the scope of Gentle Hedgehog's business?

A. Everything offered by Sauron Eye's software in relation to activity by sales team contractors. B. Everything offered by Sauron Eye's software, assuming employees provide daily consent to the monitoring. C. Only emails, website browsing history, and camera for internal video calls conducted in a non-secure environment. D. Only emails, website browsing history, and camera for internal video calls that are expressly marked as monitored.

Options:

Answer:

Explanation:

Under GDPR and EU employment law, employee monitoring must comply with the principles of necessity, proportionality, legitimacy, and transparency.

Legal requirements for employee monitoring:

Necessity: Employers must demonstrate that monitoring is necessary for a legitimate purpose.

Proportionality: The monitoring must be the least intrusive method available.

Transparency: Employees must be fully informed about what is being monitored.

Why is D the correct answer?

GDPR requires that monitoring must be explicitly communicated and justified.

Employers can monitor work emails, browsing history, and video calls, but only if employees are clearly informed and the purpose is justified.

Why are other answers incorrect?

A (Monitoring all contractor activity) Contractors have data protection rights too; monitoring must still be necessary and proportionate.

B (Daily consent requirement) Employee consent is not valid under GDPR in most cases due to power imbalance.

C (Monitoring in non-secure environments only) The location does not determine the lawfulness

of monitoring.

Conclusion: The correct answer is D, as only explicitly marked and justified monitoring is lawful under GDPR.

Question 3

Question Type: MultipleChoice

The Murla HB Club should have carried out a DPIA before the installation of the new access system AND at what other time?

A. After the complaint of the supporter B. Periodically, when new risks were foreseen C. At the end of every match of the season. D. After the AEPD notification of the investigation.

Options:

Answer:

Explanation:

A Data Protection Impact Assessment (DPIA) is required under Article 35 of the GDPR when data processing is likely to result in a high risk to individuals' rights and freedoms. This includes processing involving new technologies, systematic monitoring, or the large-scale processing of sensitive data.

When should a DPIA be conducted?

Before implementing a new high-risk processing activity (e.g., a biometric access system).

Whenever a significant change in risk occurs (e.g., security updates, regulatory changes, new threats).

Regularly to reassess and mitigate emerging risks.

Why is B the correct answer?

DPIAs are not a one-time process; they must be reviewed periodically to assess new risks.

Why are other answers incorrect?

A (After the complaint) A DPIA is a proactive measure, not something done only after a complaint.

C (At the end of the season) GDPR does not require assessments to be tied to event cycles.

D (After regulatory notification) DPIAs must be done before investigations, not as a response.

Conclusion: DPIAs should be conducted periodically when new risks arise, making B the correct answer.

Question 4

Question Type: MultipleChoice

Through a combination of hardware failure and human error, the decryption key for a bank's customer account transaction database has been lost. An investigation has determined that this was not the result of hacking or malfeasance, simply an unfortunate combination of circumstances. Which of the following accurately indicates the nature of this incident?

A. A data breach has not occurred because the loss was not the result of hacking. B. A data breach has not occurred because no data was exposed to any unauthorized individual. C. A data breach has occurred because the loss of the key has resulted in the data no longer being accessible. D. A data breach has occurred because the loss of the key has resulted in the loss of confidentiality or integrity of the data.

Options:

Answer:

Explanation:

Under the GDPR (Article 4(12)), a personal data breach is defined as:

'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed'.

Why Answer Choice D is Correct

Loss of Encryption Key = Loss of Data Availability

The loss of the decryption key means that the bank can no longer access customer transaction data.

Availability is a fundamental aspect of data security (Article 32). Loss of availability constitutes a breach under GDPR.

Loss of Confidentiality & Integrity

If the encryption key is lost, data cannot be decrypted, meaning it is effectively destroyed or altered.

This qualifies as a data breach under GDPR since data integrity and confidentiality are compromised.

Why Other Answer Choices Are Incorrect:

A (No Breach Because No Hacking):

GDPR does not require hacking for a breach to occur. A loss of access alone can qualify.

B (No Breach Because No Unauthorized Access):

Unauthorized disclosure is one type of breach, but GDPR also covers loss and destruction of personal data.

C (Data Breach Due to Inaccessibility):

Partially correct but does not fully explain the GDPR criteria. GDPR defines breaches in terms of confidentiality, integrity, and availability---all of which are affected.

Conclusion:

This incident is a data breach under GDPR, as it impacts data confidentiality, integrity, and availability.

The correct answer is D, because losing the decryption key compromises data integrity and availability, qualifying as a data breach under GDPR Article 4(12).

Question 5

Question Type: MultipleChoice

Once an organization has conducted an internal investigation to determine the scope of a ransomware attack, what is the appropriate next step in the process?

A. Assess the risks associated with the breach and, if necessary, notify affected individuals and regulatory bodies within the relevant timeframes. B. Notify law enforcement and consult with legal counsel to understand the implications of the breach and the notification requirements. C. Inform all customers and the public via social media platforms to ensure rapid dissemination of relevant information. D. Wait for law enforcement to provide guidance on notification procedures

before taking any further action.

Options:

Answer:

Explanation:

The GDPR (General Data Protection Regulation) has strict data breach response requirements, particularly for ransomware attacks that affect personal data. The appropriate next step after an internal investigation is to assess the risks associated with the breach and notify affected parties if necessary.

Key GDPR Breach Response Steps (Article 33 & 34):

Assess the risks to personal data

If the breach poses a risk to individuals' rights and freedoms, the supervisory authority (DPA) must be notified within 72 hours.

If there is a high risk, affected individuals must also be informed without undue delay.

Why Answer Choice A is Correct

Risk assessment is a critical first step after an internal investigation.

If the breach meets the risk threshold, notification to authorities and individuals is required under GDPR.

Why Other Answer Choices Are Incorrect:

B (Notify Law Enforcement First): While law enforcement may be involved, GDPR does not mandate consulting law enforcement before conducting a risk assessment or notifying individuals.

C (Informing the Public Immediately): Public disclosure via social media is not a GDPR requirement. Affected individuals and DPAs should be formally notified first.

D (Waiting for Law Enforcement): GDPR does not allow waiting for law enforcement before fulfilling notification obligations. Controllers must act within 72 hours.

Conclusion: The correct next step after an internal investigation is to assess the risks and, if necessary, notify affected individuals and regulatory bodies as required under GDPR Articles 33 and 34.

Question 6

Question Type: MultipleChoice

What is the main purpose of the EU Data Act?

A. To enable the processing and transfer of non-personal data within the EU. B. To allow users of connected devices to access data generated by their use. C. To facilitate the voluntary sharing of data between individuals and businesses. D. To regulate individuals' privacy rights and the processing of their personal data.

Options:

Answer:

Explanation:

The EU Data Act aims to increase access to data generated by connected devices (IoT devices), ensuring fair use and promoting data-driven innovation across the EU.

Key purposes of the EU Data Act:

Granting users access to data generated by their devices (Answer Choice B -- Correct Answer)

One of the Act's primary objectives is to allow users of smart devices, IoT systems, and connected industrial tools to access and control data generated by their devices.

Improving non-personal data sharing (Answer Choice A -- Incorrect)

While the Act does facilitate the transfer of non-personal data, its primary focus is on device-generated data access, rather than simply allowing free movement of non-personal data.

Encouraging data-sharing frameworks (Answer Choice C -- Incorrect)

The Act does promote data-sharing between businesses, but this is not its main goal. It primarily ensures that users retain control over data produced by their devices.

Not primarily about personal data protection (Answer Choice D -- Incorrect)

The GDPR (General Data Protection Regulation) is the primary regulation that deals with personal data protection. The Data Act does not introduce new privacy rules but instead focuses on non-personal data management.

Question 7

Question Type: MultipleChoice

According to the AI Act, a provider of a high-risk AI system has all of the following obligations EXCEPT?

A. Ensuring users understand how the system mitigates bias. B. Registering the system in the European AI Board's database. C. Providing detailed documentation about the system to the users. D. Conducting a conformity assessment before placing the system on the market.

Options:

Answer:

Explanation:

The EU Artificial Intelligence Act (AI Act) introduces strict regulations for high-risk AI systems to ensure safety, fairness, and transparency. These regulations apply to both providers and users of AI systems within the EU and even globally under certain conditions.

Key obligations for providers of high-risk AI systems under the AI Act include:

Conformity Assessment (Answer Choice D)

Before placing a high-risk AI system on the market, the provider must conduct a conformity assessment to ensure compliance with EU legal and ethical standards.

Public Registration of High-Risk AI Systems (Answer Choice B)

The AI Act requires high-risk AI systems to be registered in an EU-wide database maintained by the European Commission to enhance transparency and oversight.

Providing Documentation (Answer Choice C)

Providers must supply detailed technical documentation about the AI system to users, ensuring they understand the system's functionality, risks, and compliance measures.

Why is Answer Choice A incorrect?

The AI Act does not explicitly require providers to ensure users understand how the system mitigates bias. Instead, providers must ensure the quality of training and testing data and implement safeguards to prevent bias, but this does not extend to user education on bias

mitigation.

Question 8

Question Type: MultipleChoice

Start-up company MagicAI is developing an AI system that will be part of a medical device that detects skin cancer. To take measures against potential bias in its AI system, the IT Team decides to collect data about users' ethnic origin, nationality, and gender.

Which would be the most appropriate legal basis for this processing under the GDPR, Article 9 (Processing of special categories of personal data)?

Options:

A- Processing necessary for scientific or statistical purposes.
B- Processing necessary for reasons of substantial public interest.
C- Processing necessary for purposes of preventive or occupational medicine.
D- Processing necessary for the defense of legal claims in potential negligence cases.

Answer:

A

Explanation:

Article 9 of the GDPR outlines strict conditions for processing special categories of personal data, which includes data revealing racial or ethnic origin. While options B, C, and D might seem relevant, they don't fully align with the core purpose of MagicAI's data collection.

Here's why option A is the most appropriate:

Scientific Research: MagicAI aims to improve the accuracy and fairness of its AI system by understanding how it performs across different ethnicities, nationalities, and genders. This directly ties into scientific research aimed at improving healthcare and reducing bias in medical technology.

It's important to note that even with 'scientific research' as the legal basis, MagicAI must still adhere to strict safeguards, such as:

Data Minimization: Collecting only the data absolutely necessary for the research.

Purpose Limitation: Using the data solely for the defined scientific purpose.

Appropriate Security Measures: Protecting the data against unauthorized access or disclosure.

Ethical Review: Ideally, obtaining ethical approval for the research project.

GDPR Article 9 - Processing of special categories of personal data

GDPR Recital 159 - Conditions for processing special categories of data for scientific research purposes

IAPP CIPP/E textbook, Chapter 2: Key Data Protection Principles (specifically, sections on special categories of data)

Question 9

Question Type: MultipleChoice

SCENARIO - Please use the following to answer the next question:

It has been a tough season for the Spanish Handball League, with acts of violence and racism having increased exponentially during their last few matches.

In order to address this situation, the Spanish Minister of Sports, in conjunction with the National Handball League Association, issued an Administrative Order (the "Act") obliging all the professional clubs to install a fingerprint-reading system for accessing some areas of the sports halls, primarily the ones directly behind the goalkeepers. The rest of the areas would retain the current access system, which allows any spectators access as long as they hold valid tickets.

The Act named a selected hardware and software provider, New Digital Finger, Ltd., for the creation of the new fingerprint system. Additionally, it stipulated that any of the professional clubs that failed to install this system within a two-year period would face fines under the Act.

The Murla HB Club was the first to install the new system, renting the New Digital Finger hardware and software. Immediately afterward, the Murla HB Club automatically renewed current supporters' subscriptions, while introducing a new contractual clause requiring supporters to access specific areas of the hall through the new fingerprint reading system installed at the gates.

After the first match hosted by the Murla HB Club, a local supporter submitted a complaint to the club and to the Spanish Data Protection Authority (the AEPD), claiming that the new access system violates EU data protection laws. Having been notified by the AEPD of the upcoming investigation regarding this complaint, the Murla HB Club immediately carried out a Data Protection Impact Assessment (DPIA), the conclusions of which stated that the new access system did not pose any high risks to data subjects' privacy rights.

The Murla HB Club should have carried out a DPIA before the installation of the new access system and at what other time?

Options:

A- After the complaint of the supporter.
B- Periodically, when new risks were foreseen.
C- At the end of every match of the season.
D- After the AEPD notification of the investigation.

Answer:

B

Explanation:

A DPIA is not a one-time activity. While it's crucial to conduct a DPIA before implementing a new system that processes personal data (like the fingerprint system), the GDPR requires organizations to review and update their DPIAs periodically, especially when there are changes that might affect the risk to data subjects.

Here's why the other options are incorrect:

A . After the complaint of the supporter: While a complaint might trigger a review of the processing, the DPIA should have been done proactively before any issues arose.

C . At the end of every match of the season: This frequency is excessive and doesn't align with the idea of assessing risks when changes occur.

D . After the AEPD notification of the investigation: Similar to option A, this is reactive rather than proactive.

GDPR Article 35 - Data protection impact assessment

IAPP CIPP/E textbook, Chapter 4: Accountability and Data Governance (specifically, sections on DPIAs and ongoing review)

WP29 Guidelines on Data Protection Impact Assessment (DPIA)

Question 10

Question Type: MultipleChoice

The EDPB's Guidelines 8/2020 on the targeting of social media users stipulates that in order to rely on legitimate interest as a legal basis to process personal data, three tests must be passed. Which of the following is NOT one of the three tests?

Options:

A- Purpose test.
B- Necessity test.
C- Balancing test.
D- Adequacy test.

Answer:

D

Explanation:

The EDPB's Guidelines 8/2020 on the targeting of social media users explain that the legitimate interest legal basis requires passing three cumulative tests: the purpose test, the necessity test, and the balancing test. The purpose test checks whether there is a legitimate interest pursued by the data controller or a third party. The necessity test checks whether the processing is necessary for the purpose identified. The balancing test checks whether the legitimate interest is not overridden by the interests or rights and freedoms of the data subject. The adequacy test is not one of the three tests required by the legitimate interest legal basis. The adequacy test is relevant for data transfers to third countries, not for data processing within the EU.

EDPB Guidelines 8/2020 on the targeting of social media users, Section 3.2.11

GDPR Article 6(1)(f)2

GDPR Recital 472

IAPP CIPP/E Study Guide, Chapter 3, Section 3.2.23

Question 11

Question Type: MultipleChoice

A private company has establishments in France, Poland, the United Kingdom and, most prominently, Germany, where its headquarters is established. The company offers its services worldwide. Most of the services are designed in Germany and supported in the other establishments. However, one of the services, a Software as a Service (SaaS) application, was defined and implemented by the Polish establishment. It is also supported by the other establishments.

What is the lead supervisory authority for the SaaS service?

Options:

A- The supervisory authority of Germany at federal level.
B- The supervisory authority of Germany at regional level.
C- The supervisory authority of the Republic of Poland.
D- The supervisory authority of the European Union.

Answer:

C

Explanation:

According to the GDPR, the lead supervisory authority (LSA) is the one located in the EU member state where the controller or processor has its main establishment or single establishment. The main establishment is the place where the decisions on the purposes and means of the processing of personal data are taken. In this case, the SaaS service was defined and implemented by the Polish establishment, so the decisions on the processing of personal data for this service are taken in Poland. Therefore, the LSA for the SaaS service is the supervisory authority of the Republic of Poland.

GDPR Article 4(16): Definition of main establishment

GDPR Article 56: Competence of the lead supervisory authority

GDPR Recital 36: Determination of the main establishment

IAPP CIPP/E Study Guide, Chapter 5, Section 5.1: Lead Supervisory Authority

Question 12

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next question:

Gentle Hedgehog Inc. is a privately owned website design agency incorporated in

Italy. The company has numerous remote workers in different EU countries. Recently,

the management of Gentle Hedgehog noticed a decrease in productivity of their sales

team, especially among remote workers. As a result, the company plans to implement

a robust but privacy-friendly remote surveillance system to prevent absenteeism, reward top performers, and ensure the best quality of customer service when sales people are interacting with customers.

Gentle Hedgehog eventually hires Sauron Eye Inc., a Chinese vendor of employee surveillance software whose European headquarters is in Germany. Sauron Eye's software provides powerful remote-monitoring capabilities, including 24/7 access to computer cameras and microphones, screen captures, emails, website history, and keystrokes. Any device can be remotely monitored from a central server that is securely installed at Gentle Hedgehog headquarters. The monitoring is invisible by default; however, a so-called Transparent Mode, which regularly and conspicuously notifies all users about the monitoring and its precise scope, also exists. Additionally, the monitored employees are required to use a built-in verification technology involving facial recognition each time they log in.

All monitoring data, including the facial recognition data, is securely stored in Microsoft Azure cloud servers operated by Sauron Eye, which are physically located in France.

What is the main problem with the 24/7 camera monitoring?

Options:

A- It must not be operated during non-business hours and employee holidays.
B- It may accidentally film third parties whose consent is required for monitoring.
C- It has no valid legal basis to be implemented in the context of Gentle Hedgehog's business.
D- It must first be approved by the trade union and then granted a license from the national DPA.

Answer:

C

Explanation:

The General Data Protection Regulation (GDPR) does not prohibit surveillance of employees in the workplace. Still, it requires employers to follow special rules to ensure that the rights and freedoms of employees are protected when processing their personal data. The GDPR applies to any processing of personal data in the context of the activities of an establishment of a controller

or a processor in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.

The GDPR requires that any processing of personal data must be lawful, fair and transparent, and based on one of the six legal grounds specified in the regulation. The most relevant legal grounds for employee surveillance are the legitimate interests of the employer, the performance of a contract with the employee, or the compliance with a legal obligation. The GDPR also requires that any processing of personal data must be limited to what is necessary for the purposes for which they are processed, and that the data subjects must be informed of the purposes and the legal basis of the processing, as well as their rights and the safeguards in place to protect their data.

The GDPR also imposes specific obligations and restrictions on the processing of special categories of personal data, such as biometric data, which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or which are processed for the purpose of uniquely identifying a natural person. The processing of such data is prohibited, unless one of the ten exceptions listed in the regulation applies. The most relevant exceptions for employee surveillance are the explicit consent of the data subject, the necessity for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or the necessity for reasons of substantial public interest.

The GDPR also sets out the rules and requirements for the transfer of personal data to third countries or international organisations, which do not ensure an adequate level of data protection. The transfer of such data is only allowed if the controller or processor has provided appropriate safeguards, such as binding corporate rules, standard contractual clauses, codes of conduct or certification mechanisms, and if the data subjects have enforceable rights and effective legal remedies.

Based on the scenario, the main problem with the 24/7 camera monitoring is that it has no valid legal basis to be implemented in the context of Gentle Hedgehog's business. This option is the most consistent with the GDPR's principles and requirements, as it:

Is not based on a valid legal ground for the processing of personal data, as it does not rely on the legitimate interests of the employer, the performance of a contract with the employee, or the compliance with a legal obligation. The legitimate interests of the employer to ensure the productivity, quality and security of the work performed by the employees must be balanced with the rights and freedoms of the employees, and the 24/7 camera monitoring is likely to be disproportionate and intrusive, especially if it covers non-work-related activities and communications. The performance of a contract with the employee does not justify the 24/7 camera monitoring, as it is not necessary for the fulfilment of the contractual obligations of the employee or the employer. The compliance with a legal obligation does not apply to the 24/7 camera monitoring, as there is no specific law or regulation that requires such a measure in the context of Gentle Hedgehog's business.

Is not limited to what is necessary for the purposes of the monitoring, as it involves the collection and processing of excessive and irrelevant personal data, such as camera and microphone monitoring, which go beyond the scope of the work performed by the employees, and intrude into their private or personal sphere. The 24/7 camera monitoring is also likely to capture personal data of third parties, such as customers, suppliers or visitors, whose consent is required for the monitoring, and whose rights and freedoms may be affected by the processing.

Is not transparent to the employees, as it does not inform them of the monitoring and its precise scope, and does not give them the opportunity to object or opt out of the monitoring. The monitoring is invisible by default, which means that the employees are not aware of when and how they are being monitored, and what personal data are being collected and processed. The so-called Transparent Mode, which regularly and conspicuously notifies all users about the monitoring and its precise scope, is also insufficient, as it does not provide the employees with a clear and comprehensive information notice, nor with a valid and specific consent form, as required by the GDPR.

Involves the processing of special categories of personal data, such as biometric data or data revealing political opinions or trade union membership, which are not necessary or proportionate for the purposes of the monitoring, and which do not fall under any of the exceptions listed in the regulation. The facial recognition technology used by the monitoring system is a form of biometric data processing, which is prohibited by the GDPR, unless the data subject has given explicit consent, or the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or the processing is necessary for reasons of substantial public interest. None of these exceptions apply to the scenario, as the facial recognition technology is not used for any of these purposes, but rather for verifying the identity of the employees each time they log in. The camera and microphone monitoring may also capture personal data revealing political opinions or trade union membership, which are also special categories of personal data, and which are not relevant or proportionate for the purposes of the monitoring.

Involves the transfer of personal data to a third country, such as China, which does not provide an adequate level of data protection, and which may pose additional risks for the rights and freedoms of the employees. The monitoring data, including the facial recognition data, are securely stored in Microsoft Azure cloud servers operated by Sauron Eye, which are physically located in France. However, Sauron Eye is a Chinese vendor of employee surveillance software, whose European headquarters is in Germany. This means that the monitoring data may be accessed or transferred by Sauron Eye to its parent company or other affiliates in China, which is a third country that does not ensure an adequate level of data protection, according to the European Commission. The transfer of personal data to China is only allowed if the controller or processor has provided appropriate safeguards, such as binding corporate rules, standard contractual clauses, codes of conduct or certification mechanisms, and if the data subjects have enforceable rights and effective legal remedies. However, the scenario does not indicate that any of these safeguards or remedies are in place, and therefore the transfer of personal data to China may violate the GDPR.

The other options listed in the question are not the main problem with the 24/7 camera monitoring, as they:

Are not directly related to the GDPR's principles and requirements, but rather to the national laws and regulations of the member states, which may vary depending on the specific context and circumstances of the monitoring. The GDPR does not specify a precise time limit for the operation of the camera monitoring, but leaves it to the national laws and regulations of the member states to determine the appropriate conditions and safeguards for the monitoring, taking into account the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of data subjects. The GDPR also does not require the approval of the trade union or the license from the national DPA for the camera monitoring, but leaves it to the national laws and regulations of the member states to establish the appropriate procedures and mechanisms for the consultation and involvement of the relevant stakeholders, such as the employees, the trade unions, the works councils, the DPAs or the courts.

Are not the main problem with the 24/7 camera monitoring, but rather the consequences or the implications of the main problem, which is the lack of a valid legal basis for the monitoring. The operation of the camera monitoring during non-business hours and employee holidays, or the accidental filming of third parties whose consent is required for the monitoring, are not the main problem, but rather the result of the main problem, which is the excessive and disproportionate collection and processing of personal data, which go beyond the scope of the work performed by the employees, and intrude into their private or personal sphere. The approval of the trade union or the license from the national DPA are not the main problem, but rather the potential solutions or remedies for the main problem, which is the absence of transparency and accountability for the monitoring, which do not inform the employees of the monitoring and its precise scope, and do not give them the opportunity to object or opt out of the monitoring.

GDPR, Articles 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 44, 45, 46, 47, 48, and 49.

EDPB Guidelines 3/2019 on processing of personal data through video devices, pages 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14.

[EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR]

To Get Premium Files for CIPP-E Visit
https://www.p2pexams.com/products/cipp-e

For More Free Questions Visit
https://www.p2pexams.com/iapp/pdf/cipp-e

