



# CIPP-E<sup>Q&As</sup>

Certified Information Privacy Professional/Europe (CIPP/E)

**Pass IAPP CIPP-E Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/cipp-e.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

After detecting an intrusion involving the theft of unencrypted personal data, who shall the breached company notify first under GDPR requirements?

- A. Any parents of children whose personal data was compromised.
- B. Any affected customers whose data was compromised.
- C. A competent supervisory authority.
- D. A local law enforcement agency

Correct Answer: C

---

**QUESTION 2**

To comply with the GDPR and the EU Court of Justice's decision in Schrems II, the European Commission issued what are commonly referred to as the new standard contractual clauses (SCCs). As a result, businesses must do all of the following EXCEPT?

- A. Consider the new optional docking clause, which expressly permits adding new parties to the SCCs.
- B. Migrate all contracts entered into before September 27, 2021, that use the old SCCs to the new SCCs by December 27, 2022.
- C. Take steps to flow down the new SCCs to relevant parts of their supply chain using the new SCCs as of September 27, 2021, if the business is a data importer.
- D. Implement the new SCCs in the U.K. following Brexit, as the U.K. Information Commissioner's Office does not have the authority to publish its own set of SCCs.

Correct Answer: D

---

**QUESTION 3**

Which of the following is an accurate statement regarding the "one-stop-shop" mechanism of the GDPR?

- A. It can result in several lead supervisory authorities in the EU assuming competence over the same data processing activities of an organization.
- B. It applies only to direct enforcement of data protection supervisory authorities (e.g., finding a breach), but not to initiating or engaging in court proceedings
- C. It gives competence to the lead supervisory authority to address privacy issues derived from processes carried out by public authorities established in different countries.



D. It allows supervisory authorities concerned (other than the lead supervisory authority) to act against organizations in exceptional cases even if they do not have any type of establishment in the Member State of the respective authority.

Correct Answer: D

---

#### QUESTION 4

##### SCENARIO

Please use the following to answer the next question:

Financially, it has been a very good year at ARRA Hotels: Their 21 hotels, located in Greece (5), Italy (15) and Spain (1), have registered their most profitable results ever. To celebrate this achievement, ARRA Hotels' Human Resources office, based in ARRA's main Italian establishment, has organized a team event for its 420 employees and their families at its hotel in Spain.

Upon arrival at the hotel, each employee and family member is given an electronic wristband at the reception desk. The wristband serves a number of functions:

1.  
Allows access to the "party zone" of the hotel, and emits a buzz if the user approaches any unauthorized areas
2.  
Allows up to three free drinks for each person of legal age, and emits a buzz once this limit has been reached
3.  
Grants a unique ID number for participating in the games and contests that have been planned.

Along with the wristband, each guest receives a QR code that leads to the online privacy notice describing the use of the wristband. The page also contains an unchecked consent checkbox. In the case of employee family members under the age of 16, consent must be given by a parent. Among the various activities planned for the event, ARRA Hotels' HR office has autonomously set up a photocall area, separate from the main event venue, where employees can come and have their pictures taken in traditional carnival

costume. The photos will be posted on ARRA Hotels' main website for general marketing purposes.

On the night of the event, an employee from one of ARRA's Greek hotels is displeased with the results of the photos in which he appears. He intends to file a complaint with the relevant supervisory authority in regard to the following:

1.  
The lack of any privacy notice in the separate photocall area
2.  
The unlawful cross-border processing of his personal data
- 3.



The unacceptable aesthetic outcome of his photos

Assuming that there is a cross-border processing of personal data, which of the following criteria would NOT be useful to the lead supervisory authority responsible for the Greek employee's complaint when trying to determine the location of the controller's main establishment?

- A. Where the controller is registered as a company.
- B. Where the processor is registered as a company.
- C. Where decisions about the processing activities are made.
- D. Where the director with responsibility for processing activities is located.

Correct Answer: B

---

#### QUESTION 5

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.

Correct Answer: D

Reference: <https://www.futurelearn.com/courses/general-data-protection-regulation/0/steps/32449>

---

#### QUESTION 6

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.

Correct Answer: D



## QUESTION 7

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.

Correct Answer: A

Reference: <https://dataprivacymanager.net/sensitive-personal-data-special-category-under-the-gdpr/>

---

## QUESTION 8

### 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 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.

Correct Answer: C

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

---

## QUESTION 9

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

- A. Everything offered by Sauron Eye's software with the exception of camera and microphone monitoring.



- B. Everything offered by Sauron Eye's software, assuming employees provide daily consent to the monitoring.
- C. Only video calls conducted during business hours and emails that do not contain a "private" or "personal" tag.
- D. Only emails, website browsing history and camera for internal video calls that are expressly marked as monitored.

Correct Answer: D

---

#### QUESTION 10

The origin of privacy as a fundamental human right can be found in which document?

- A. Universal Declaration of Human Rights 1948.
- B. European Convention of Human Rights 1953.
- C. OECD Guidelines on the Protection of Privacy 1980.
- D. Charter of Fundamental Rights of the European Union 2000.

Correct Answer: A

---

#### QUESTION 11

A company wishes to transfer personal data to a country outside of the European Union/EEA. In order to do so, they are planning an assessment of the country's laws and practices, knowing that these may impinge upon the transfer safeguards they intend to use.

All of the following factors would be relevant for the company to consider EXCEPT?

- A. Any onward transfers, such as transfers of personal data to a sub-processor in the same or another third country.
- B. The process of modernization in the third country concerned and their access to emerging technologies that rely on international transfers of personal data.
- C. The technical, financial, and staff resources available to an authority in the third country concerned that may access the personal data to be transferred.
- D. The contractual clauses between the data controller or processor established in the European Union/EEA and the recipient of the transfer established in the third country concerned.

Correct Answer: B

---

#### QUESTION 12

The transparency principle is most directly related to which of the following rights?

- A. Right to object



- B. Right to be informed.
- C. Right to be forgotten.
- D. Right to restriction of processing.

Correct Answer: B

---

#### QUESTION 13

In which case would a controller who has undertaken a DPIA most likely need to consult with a supervisory authority?

- A. Where the DPIA identifies that personal data needs to be transferred to other countries outside of the EEA.
- B. Where the DPIA identifies high risks to individuals' rights and freedoms that the controller can take steps to reduce.
- C. Where the DPIA identifies that the processing being proposed collects the sensitive data of EU citizens.
- D. Where the DPIA identifies risks that will require insurance for protecting its business interests.

Correct Answer: B

Reference: <https://www.dataguidance.com/opinion/eu-how-when-and-why-carrying-out-dpia>

---

#### QUESTION 14

If a company chooses to ground an international data transfer on the contractual route, which of the following is NOT a valid set of standard contractual clauses?

- A. Decision 2001/497/EC (EU controller to non-EU or EEA controller).
- B. Decision 2004/915/EC (EU controller to non-EU or EEA controller).
- C. Decision 2007/72/EC (EU processor to non-EU or EEA controller).
- D. Decision 2010/87/EU (Non-EU or EEA processor from EU controller).

Correct Answer: C

---

#### QUESTION 15

If two controllers act as joint controllers pursuant to Article 26 of the GDPR, which of the following may NOT be validly determined by said controllers?

- A. The definition of a central contact point for data subjects.
- B. The rules regarding the exercising of data subjects' rights.
- C. The rules to provide information to data subjects in Articles 13 and 14.





D. The non-disclosure of the essence of their arrangement to data subjects

Correct Answer: D

[Latest CIPP-E Dumps](#)

[CIPP-E VCE Dumps](#)

[CIPP-E Practice Test](#)