



CIPP-E^{Q&As}

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

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.

Correct Answer: C

QUESTION 2

What is the most frequently used mechanism for legitimizing cross-border data transfer?

A. Standard Contractual Clauses.

B. Approved Code of Conduct.

C. Binding Corporate Rules.

D. Derogations.

Correct Answer: A

Reference: <https://www.dataguidance.com/opinion/international-eu-us-cross-border-data-transfers>

QUESTION 3

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

Correct Answer: B

QUESTION 4

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.

Correct Answer: B



QUESTION 5

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.

Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?

- 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.

Correct Answer: C