

CIPP/E

CERTIFIED INFORMATION PRIVACY
PROFESSIONAL/EUROPE

PRACTICE EXAM QUESTIONS

SIMILAR EXAM QUESTIONS

*Are you **determined** to pass the exam?
then get the **full version** of this ebook!*

**FREE
SAMPLE**

PREPARED BY CIPP/E, CISA, MSC EXPERTS

THIS IS NOT AN OFFICIAL IAPP MATERIAL

COPYRIGHT © CERTIFICATION EXAM TRAINER. ALL RIGHTS RESERVED

Introduction:

Welcome to the CIPP/E Practice Exam Book! This **sample** book is here to help you prepare for the Certified Information Privacy Professional/Europe (CIPP/E) certification exam, which is administered by the International Association of Privacy Professionals (IAPP). Whether you're already working in privacy or just starting out, this book is designed to support you in getting ready for the exam.

The aim of this practice exam is not just to test whether you've memorized your study material, but also to assess your ability to apply it – a crucial aspect of passing the exam successfully.

Use this practice exam as a tool to gauge your understanding, identify areas of strength and weakness, and fine-tune your exam strategy. Remember, practice and application are key to success.

How to Take This Practice Exam:

This e-book contains a brief subset of 10 questions from the CIPP/E Privacy Exam questions. The original book contains 156 questions, distributed between direct questions and 13 scenarios. The target to aim for is an 80% score, meaning you should aim to have 30 mistakes or fewer in order to be confident in your readiness for the exam. If you score 80% or higher, you can consider yourself well-prepared for exam day.

- **Gather Your Materials:** Get a piece of paper, a pencil, and a timer.
- **Set a Timer:** Set a timer for 2.5 hours and aim to resolve 90 questions (as the actual exam). This will simulate the time constraint of the actual exam.
- **Answering Questions:** Write down the number of each question and the answer you believe is correct. If you're unsure about an answer or want to review it later, mark it with a question mark. This helps you flag questions for review without wasting time.
- **Flagging for Review:** Mark the question you want to review later. This technique can be helpful during the actual exam as well.
- **Refer to Answer Key:** After completing the exam or when the timer runs out, refer to the answer key provided in this booklet to determine your score.

- **Understanding the Logic:** Take time to understand the reasoning behind each question and answer. This is crucial for learning and improving your understanding of the material.
- **Reviewing Explanations:** In the last section of this booklet, explanations are provided for each question. Use these explanations to deepen your understanding of the concepts tested.

By following these steps, you'll not only assess your readiness for the exam but also enhance your knowledge and test-taking skills.

About This Book:

Unlike the current practice exams available, which are often out-of-date, expensive, and too easy, this practice exam booklet offers a more challenging and realistic experience. With brief explanations provided, you'll gain insight into question phrasing and learn how to select the best answer.

Note: This is not an official CIPP/e sample exam, nor does it contain real exam questions. However, it provides similar questions and degree of difficulty as the real exam.

By using this booklet alongside your regular study material, you'll not only enhance your speed and accuracy but also have ample time to review flagged questions. The variety of question types in this practice exam mirrors the actual exam, ensuring a balanced approach to testing your knowledge.

For those seeking to further test their GDPR application skills, consider trying out this book. This resource focuses specifically on scenario-based questions, which are often the most difficult part of the exam, providing an additional challenge to assess your understanding of the European Privacy Law.

Best of luck in your preparations!

Note: This e-book is protected by copyright law. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, distribution, or resale of this eBook is strictly prohibited. Legal action will be taken against individuals or entities found to be in violation of these restrictions.

Table of Contents

Introduction:..... 1

About This Book: 2

 CIPP/E Practice Exam Questions..... 4

 CIPP/E Practice Exam Answers & Explanations 7

CIPP/E Practice Exam Questions

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 insurer upon request.

2. SCENARIO

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.

3. SCENARIO

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.

4. 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

5. How does the GDPR now define "processing"?

- A. Any act involving the collecting and recording of personal data.
- B. Any operation or set of operations performed on personal data or on sets of personal data.
- C. Any use or disclosure of personal data compatible with the purpose for which the data was collected.
- D. Any operation or set of operations performed by automated means on personal data or on sets of personal data.

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

- A. The controller will be liable to pay an administrative fine

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

7. According to the GDPR, how is pseudonymous personal data defined?

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

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

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

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

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

10. What type of data lies beyond the scope of the General Data Protection Regulation?

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

Interested in more similar exam questions? Then obtain the full e-book with more than 150 similar exam questions and answers!

CIPP/E Practice Exam Answers & Explanations

1. A. Bedrock does not have a duty to transfer Louis's data to Zantrum if doing so is legitimately not technically feasible.

Explanation: According to the GDPR, if it is not technically feasible to transfer a data subject's data to another organization, the organization may not have a duty to do so, as long as they provide the data subject with their data in a commonly used, machine-readable format.

2. C. If the data becomes necessary to defend Accidentable's legal rights.

Explanation: Accidentable may have grounds for refusing to comply with Louis's request to restrict the use of his data if the data becomes necessary for the defense of Accidentable's legal rights.

3. 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.

Explanation: Under the GDPR, data subjects have the right to object at any time to the processing of their personal data for direct marketing purposes. Bedrock Insurance must honor Louis's request to cease using his data for marketing purposes, even if he had previously consented to it. Consent should be freely given and can be withdrawn at any time without detriment.

4. C. Where the decisions about processing are made.

Explanation: According to the E-Commerce Directive 2000/31/EC and the GDPR, the place of "establishment" for a company providing services via an Internet website is confirmed by where the decisions about processing are made. This means that the location where the key decisions regarding data processing activities are made determines the applicability of the GDPR.

5. B. Any operation or set of operations performed on personal data or on sets of personal data.

Explanation: The GDPR defines "processing" as any operation or set of operations performed on personal data or on sets of personal data. This definition is broad and covers various activities related to personal data, including collection, storage, retrieval, use, and more.

6. C. The processor will be considered to be a controller in respect of the processing concerned.

Explanation: If a processor makes an independent decision regarding the purposes and means of processing it carries out on behalf of a controller, the processor may be considered a controller in respect of the processing concerned. This can lead to legal complications and responsibilities under the GDPR.

7. A. Data that can no longer be attributed to a specific data subject without the use of additional information kept separately.

Explanation: Pseudonymous personal data, as defined by the GDPR, is data that can no longer be attributed to a specific data subject without the use of additional information kept separately. It allows for a level of data protection while not completely anonymizing the data.

8. C. The unlinked aggregated data used for statistical purposes by an Italian company.

Explanation: Unlinked aggregated data used for statistical purposes, where individual data subjects cannot be identified, is less likely to be covered by the definition of "personal data" under the GDPR. Personal data typically relates to information that can identify individuals.

9. D. Personal data of EU residents being processed by a non-EU business that targets EU customers.

Explanation: The extraterritorial effect of the GDPR, as specified by Article 3, is triggered when personal data of EU residents is processed by a non-EU business that targets EU customers. This means that businesses outside the EU that offer goods or services to EU residents must comply with the GDPR.

10. B. Anonymized

Explanation: Anonymized data, which is data that has been processed in such a way that it can no longer be used to identify an individual, falls outside the scope of the GDPR because it no longer qualifies as personal data.