ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: IAPP

Code: CIPP-E

Exam: Certified Information Privacy Professional/Europe

https://www.examsnest.com/exam/cipp-e/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 8.5

Question: 1

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.

Answer: D

Explanation:

A data breach is broadly defined as any incident that leads to the unauthorized access, disclosure, alteration, or destruction of personal data. While options A and B might seem plausible at first glance, they focus on a narrow interpretation of a breach.
The key here is the loss of confidentiality and/or integrity. Even though no one has actively stolen the data, the bank can no longer guarantee the confidentiality of the information, nor can it ensure the integrity of the data since it cannot be accessed or modified securely. This constitutes a loss of control over the data and thus qualifies as a data breach.
Reference:
IAPP CIPP/E textbook, Chapter 5: Data Breach Notification (specifically, the definition of a personal data breach)
GDPR Article 4(12) - Definition of a personal data breach

Question: 2

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?

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

Answer: C

Explanation:

Under the GDPR, the lead supervisory authority is determined by where the main establishment related to the processing activity is located.
In this case, even though the company's headquarters is in Germany, the SaaS application was specifically defined and implemented by the Polish establishment. This indicates that the Polish establishment has the primary role in determining the purposes and means of processing personal data related to that SaaS service. Therefore, the supervisory authority of Poland would be the lead supervisory authority for this specific processing activity.
Reference:
GDPR Article 56 - Competence of the lead supervisory authority
IAPP CIPP/E textbook, Chapter 3: EU General Data Protection Regulation (specifically, sections on One-Stop Shop mechanism and lead supervisory authority)

Question: 3

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

Answer: B

Explanation:
Article 8 of the ECHR protects the right to respect for private and family life, home and correspondence. However, this right is not absolute and can be subject to limitations by a public authority in accordance with the law and for a legitimate aim. The European Court of Human Rights (ECtHR) has developed a two-stage test to determine whether such limitations are justified. First, the court must examine whether there is a legitimate aim pursued by the public authority, such as national security, public safety or the prevention of crime. Second, the court must assess whether the means used by the public authority are appropriate and necessary to achieve that aim, taking into account all relevant factors such as proportionality, necessity and less restrictive alternatives12. Therefore, the right to privacy is not an absolute right but a qualified one that has to be balanced against other rights under the ECHR. Reference:
Article 8 - Protection of personal data
Your right to respect for private and family life
Right to respect for private and family life
Guide on Article 8 of the European Convention on Human Rights
European Convention on Human Rights - Article 8

Reference: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf (15)

Question: 4

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

Answer: C

Explanation:
The OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) all aimed to harmonize the national data protection laws of the member states of the European Economic

Community (EEC) and to establish a common framework for the protection of personal data. However, they largely failed to achieve this goal due to several reasons, such as:
The lack of political will and commitment from the member states to implement the directives fully and consistently12.
The divergent interpretations and applications of the directives by different national authorities, courts and regulators12.
The emergence of new technologies and challenges that required new or updated legal solutions, such as electronic communications, cookies, biometrics, cloud computing, etc12.
The influence of other regional or international initiatives that addressed some aspects of data protection differently or in conflict with the directives, such as the US Privacy Shield Framework3.
Reference: 1: Free CIPP/E Study Guide - International Association of Privacy Professionals 2: CIPP/E Certification - International Association of Privacy Professionals 3: Schrems II: A Critical Analysis - European Data Protection Board

Reference: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf (99)

Question: 5

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

Answer: D

Explanation:
: The Individual Participation Principle is one of the Fair Information Practice Principles (FIPPs) that are not part of any legal framework, but are widely adopted by many data privacy regulations in force today1. The FIPPs are a set of guidelines for fair information practices that aim to protect the privacy and security of personal information. The Individual Participation Principle holds that individuals have a number of rights, including the right to have their personal data corrected or erased, the right to access and obtain confirmation of their personal data, the right to be informed about how their personal data is used and who it is shared with, and the right to object or withdraw consent for certain purposes2.
The General Data Protection Regulation (GDPR) is a legal framework that implements the European Union's (EU) Data Protection Directive and provides comprehensive protection for all individuals within the EU regarding their personal data. The GDPR grants individuals a number of rights, such as the right to access, rectify, erase, restrict, port, object, or not be subject to automated decision-making based on

their personal data. These rights are similar to those under the FIPPs and can be found in Articles 12 to 22 of the GDPR.
Therefore, the parts of the GDPR that provide the closest equivalent to the Individual Participation Principle are Articles 12 to 22.
Reference:
OECD Privacy Principles
What are the 7 main principles of GDPR?
Fair Information Practice Principles (FIPPs)
Individual Participation - International Association of Privacy Professionals
What is the right to be forgotten? | Right to erasure | Cloudflare
General Data Protection Regulation - Wikipedia

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: IAPP

Code: CIPP-E

Exam: Certified Information Privacy Professional/Europe

https://www.examsnest.com/exam/cipp-e/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation