CIPP/E PRACTICE EXAM

An iapp publication

CIPP/E® Practice Exam

An IAPP Publication

v1.2

About the IAPP CIPP/E Practice Exam

The IAPP CIPP/E practice exam is designed to support your preparation for the CIPP/E certification exam. Developed using IAPP study resources as well as subject matter experts' practical knowledge of the topics set forth in the IAPP's CIPP/E body of knowledge, the practice exam can help identify your relative strengths and weaknesses in the major domains of the CIPP/E body of knowledge. It was developed to simulate the types and breadth of questions you may encounter on the CIPP/E certification exam and is intended for use as an aide to focus study.

A strong performance on the practice exam does not guarantee similar success on the certification exam.

All items on the IAPP CIPP/E practice exam were reviewed for accuracy at the time of publication.

The IAPP CIPP/E practice exam was developed independently of the CIPP/E certification exam and does not contain CIPP/E certification exam items in active use.

Do you have questions or comments?
Please contact us at training@iapp.org

Table of Contents

Instructions

1. Print out the answer sheet that precedes the exam. Use this to indicate your selection for each question. If you prefer, you may use the highlighter feature of your PDF reader to indicate your response.

2. To simulate the certification exam, set a timer for 150 minutes (2.5 hours).

3. Complete the test without referring to the answer key or rationales.

4. Print out the three-page answer key which follows the exam. Check your answers against the answer key.

5. For each correct response, place a "1" or a checkmark in the corresponding domain column of the answer key. Note, the domain is indicated by an unshaded box and corresponds to the domain listed in the body of knowledge. The letter in the box next to the unshaded box is the sub-domain of the body of knowledge to which the question relates.

6. Add up the number of correct answers under each domain column.

7. To compare how you did in each domain, calculate your scores as a percent:
    a. Divide the number of correct answers by the total number of questions in that domain.
    b. Multiply that number by 100.

8. Consult the rationales for detailed explanations of each answer and the section of the body of knowledge to which the question relates.

Answer Sheet

1 Ⓐ Ⓑ Ⓒ Ⓓ	2 Ⓐ Ⓑ Ⓒ Ⓓ	3 Ⓐ Ⓑ Ⓒ Ⓓ	4 Ⓐ Ⓑ Ⓒ Ⓓ	5 Ⓐ Ⓑ Ⓒ Ⓓ
6 Ⓐ Ⓑ Ⓒ Ⓓ	7 Ⓐ Ⓑ Ⓒ Ⓓ	8 Ⓐ Ⓑ Ⓒ Ⓓ	9 Ⓐ Ⓑ Ⓒ Ⓓ	10 Ⓐ Ⓑ Ⓒ Ⓓ
11 Ⓐ Ⓑ Ⓒ Ⓓ	12 Ⓐ Ⓑ Ⓒ Ⓓ	13 Ⓐ Ⓑ Ⓒ Ⓓ	14 Ⓐ Ⓑ Ⓒ Ⓓ	15 Ⓐ Ⓑ Ⓒ Ⓓ
16 Ⓐ Ⓑ Ⓒ Ⓓ	17 Ⓐ Ⓑ Ⓒ Ⓓ	18 Ⓐ Ⓑ Ⓒ Ⓓ	19 Ⓐ Ⓑ Ⓒ Ⓓ	20 Ⓐ Ⓑ Ⓒ Ⓓ
21 Ⓐ Ⓑ Ⓒ Ⓓ	22 Ⓐ Ⓑ Ⓒ Ⓓ	23 Ⓐ Ⓑ Ⓒ Ⓓ	24 Ⓐ Ⓑ Ⓒ Ⓓ	25 Ⓐ Ⓑ Ⓒ Ⓓ
26 Ⓐ Ⓑ Ⓒ Ⓓ	27 Ⓐ Ⓑ Ⓒ Ⓓ	28 Ⓐ Ⓑ Ⓒ Ⓓ	29 Ⓐ Ⓑ Ⓒ Ⓓ	30 Ⓐ Ⓑ Ⓒ Ⓓ
31 Ⓐ Ⓑ Ⓒ Ⓓ	32 Ⓐ Ⓑ Ⓒ Ⓓ	33 Ⓐ Ⓑ Ⓒ Ⓓ	34 Ⓐ Ⓑ Ⓒ Ⓓ	35 Ⓐ Ⓑ Ⓒ Ⓓ
36 Ⓐ Ⓑ Ⓒ Ⓓ	37 Ⓐ Ⓑ Ⓒ Ⓓ	38 Ⓐ Ⓑ Ⓒ Ⓓ	39 Ⓐ Ⓑ Ⓒ Ⓓ	40 Ⓐ Ⓑ Ⓒ Ⓓ
41 Ⓐ Ⓑ Ⓒ Ⓓ	42 Ⓐ Ⓑ Ⓒ Ⓓ	43 Ⓐ Ⓑ Ⓒ Ⓓ	44 Ⓐ Ⓑ Ⓒ Ⓓ	45 Ⓐ Ⓑ Ⓒ Ⓓ
46 Ⓐ Ⓑ Ⓒ Ⓓ	47 Ⓐ Ⓑ Ⓒ Ⓓ	48 Ⓐ Ⓑ Ⓒ Ⓓ	49 Ⓐ Ⓑ Ⓒ Ⓓ	50 Ⓐ Ⓑ Ⓒ Ⓓ
51 Ⓐ Ⓑ Ⓒ Ⓓ	52 Ⓐ Ⓑ Ⓒ Ⓓ	53 Ⓐ Ⓑ Ⓒ Ⓓ	54 Ⓐ Ⓑ Ⓒ Ⓓ	55 Ⓐ Ⓑ Ⓒ Ⓓ
56 Ⓐ Ⓑ Ⓒ Ⓓ	57 Ⓐ Ⓑ Ⓒ Ⓓ	58 Ⓐ Ⓑ Ⓒ Ⓓ	59 Ⓐ Ⓑ Ⓒ Ⓓ	60 Ⓐ Ⓑ Ⓒ Ⓓ
61 Ⓐ Ⓑ Ⓒ Ⓓ	62 Ⓐ Ⓑ Ⓒ Ⓓ	63 Ⓐ Ⓑ Ⓒ Ⓓ	64 Ⓐ Ⓑ Ⓒ Ⓓ	65 Ⓐ Ⓑ Ⓒ Ⓓ
66 Ⓐ Ⓑ Ⓒ Ⓓ	67 Ⓐ Ⓑ Ⓒ Ⓓ	68 Ⓐ Ⓑ Ⓒ Ⓓ	69 Ⓐ Ⓑ Ⓒ Ⓓ	70 Ⓐ Ⓑ Ⓒ Ⓓ
71 Ⓐ Ⓑ Ⓒ Ⓓ	72 Ⓐ Ⓑ Ⓒ Ⓓ	73 Ⓐ Ⓑ Ⓒ Ⓓ	74 Ⓐ Ⓑ Ⓒ Ⓓ	75 Ⓐ Ⓑ Ⓒ Ⓓ
76 Ⓐ Ⓑ Ⓒ Ⓓ	77 Ⓐ Ⓑ Ⓒ Ⓓ	78 Ⓐ Ⓑ Ⓒ Ⓓ	79 Ⓐ Ⓑ Ⓒ Ⓓ	80 Ⓐ Ⓑ Ⓒ Ⓓ
81 Ⓐ Ⓑ Ⓒ Ⓓ	82 Ⓐ Ⓑ Ⓒ Ⓓ	83 Ⓐ Ⓑ Ⓒ Ⓓ	84 Ⓐ Ⓑ Ⓒ Ⓓ	85 Ⓐ Ⓑ Ⓒ Ⓓ
86 Ⓐ Ⓑ Ⓒ Ⓓ	87 Ⓐ Ⓑ Ⓒ Ⓓ	88 Ⓐ Ⓑ Ⓒ Ⓓ	89 Ⓐ Ⓑ Ⓒ Ⓓ	90 Ⓐ Ⓑ Ⓒ Ⓓ

CIPP/E Practice Exam

1. How does the GDPR 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.

2. A breach of security leading to the accidental destruction or loss of personal data triggers notification obligations. According to Article 33(2) of the GDPR, how soon must the data processor notify the data controller about such breach of security?

   A. Within 48 hours after the breach of security took place.
   B. Timing will vary based upon the data processing agreement.
   C. Without undue delay after becoming aware of the personal data breach.
   D. Timing will vary depending on the laws of the country where the data controller operates its primary business.

3. Under the GDPR, when processing an individual's personal data in the context of direct marketing activities, data controllers must do which of the following?

   A. Provide individuals with the categories of any third parties who will rely on the consent.
   B. Encrypt the personal data being processed prior to using it for marketing purposes.
   C. Disclose to individuals the specific lawful basis for the collection and use of the personal data.
   D. Provide individuals with information explaining that their personal data will be used for marketing purposes.

4. A full and valid set of binding corporate rules (BCRs) must include specific elements. Which of the following is **NOT** one of the required elements?

   A. A list of the specific categories of personal data to be processed under the BCR.
   B. A list of all controllers and processors for data transfers not affected by the BCR.
   C. A list of the methods through which the BCRs are communicated to data subjects.
   D. A list of the tasks of any person in charge of monitoring compliance with the BCR.

5. What is an important difference between the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) in relation to their roles and functions?

   A. ECHR can rule on issues concerning privacy as a fundamental right, while the CJEU cannot.
   B. CJEU can force national governments to implement and honour EU law, while the ECHR cannot.
   C. CJEU can hear appeals on human rights decisions made by national courts, while the ECHR cannot.
   D. ECHR can enforce human rights laws against governments that fail to implement them, while the CJEU cannot.

6. According to GDPR Article 56, what is a lead supervisory authority's (LSA) main concern?

   A. Data subject rights.
   B. Data access disputes.
   C. Cross-border processing.
   D. Special categories of data.

7. Which of the following would **most likely** trigger the extraterritorial effect of the GDPR, as specified by Article 3?

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

8. Each of the following is a valid transfer mechanism data controllers may rely upon to legally transfer EU personal data outside of the EU EXCEPT?

   A. Industry standards.
   B. Binding corporate rules.
   C. Adequacy determination.
   D. Standard contractual clauses.

9. Which of the following is **NOT** amongst the rights and freedoms that must be considered when balancing privacy rights under the GDPR?

   A. Right to a fair trial.
   B. Freedom of expression.
   C. Right to self-determination.
   D. Freedom to conduct a lawful business.

10. A high-security bank requires members to use fingerprint identification to access specific vaults. The bank retains those records to determine who obtained access and when. The bank must determine the lawful basis for processing under the GDPR.

    Which lawful basis would **most likely** apply to this type of processing activity?

    A. The bank must require members to provide consent to the processing of their fingerprints for the purposes of uniquely identifying them according to Article 9(2)(a) and disclose the purpose for the collection.
    B. The bank must have a legitimate interest for processing, must meet with a condition of processing under Article 9(2) and undertake a balance test with the fundamental rights and freedoms of the data subject.
    C. The bank must rely on processing for the carrying out of obligations if authorised by member state law under Article 9(2)(b) and proceed with conducting a data protection impact assessment.
    D. The bank must halt the implementation altogether since Article 9(1) prohibits organisations from collecting and processing biometric data for the purpose of uniquely identifying their members.

11. Administrative fines imposed under GDPR Article 83 must be?

    A. Transparent, fair, and accountable.
    B. Punitive, exemplary, and newsworthy.
    C. Reasonable, appropriate, and pertinent.
    D. Effective, proportionate, and dissuasive.

12. Much of the GDPR builds upon the Data Protection Directive. Which of the following data subject rights is the only right that did **NOT** exist in some form in the Directive?

    A. The right of access.
    B. The right to rectification.
    C. The right to data portability.
    D. The right to restrict processing.

SCENARIO I
Please use the following scenario to answer the next THREE questions.

Building Block Inc. is a multinational company headquartered in Chicago with offices throughout the United States, Asia and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their privacy office and the information security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's privacy office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the security team on how to use SecurityScan to monitor employees' computer activity and their location. During these activities, the information security team discovered that one employee from Italy was connecting daily to a video library of movies and another from Germany worked remotely without authorisation. The security team reported these incidents to the privacy office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.

Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees since the security and privacy policy of the company prohibited employees from installing software on the company's computers and from working remotely without authorisation.

13. To comply with the GDPR, what should Building Block have done as a first step before implementing the SecurityScan measure?

    A. Consulted with the relevant data protection authority about potential privacy violations.
    B. Assessed potential privacy risks by conducting a data protection impact assessment.
    C. Distributed a more comprehensive notice to employees and received their express consent.
    D. Consulted with the information security team to weigh security measures against possible server impacts.

14. What would be the most appropriate way for Building Block to handle the situation with the employee from Italy?

    A. Since the GDPR does not apply to this situation, the company would be entitled to apply any disciplinary measure authorised under Italian labour law.
    B. Since the employee was the cause of a serious risk for the server performance and company data, the company would be entitled to apply disciplinary measures to this employee, including fair dismissal.
    C. Since the employee was not informed that the security measures would be used for other purposes such as monitoring, the company could face difficulties in applying any disciplinary measures to this employee.
    D. Since this was a serious infringement, but the employee was not appropriately informed about the consequences of the new security measures, the company would be entitled to apply some disciplinary measures but not dismissal.

15. In addition to notifying employees about the purpose of the monitoring, the potential uses of their data and their privacy rights, what information should Building Block have provided them before implementing the security measures?

    A. Information about what is specified in the employment contract.
    B. Information about whom employees should contact for any queries.
    C. Information about how providing consent could affect them as employees.
    D. Information about how the measures are in the best interests of the company.

END OF SCENARIO I QUESTIONS

16. Which of the following would most likely **NOT** be covered by the definition of 'personal data' under the GDPR?

    A. A payment card number of a Dutch citizen.
    B. A U.S. Social Security number of an American citizen living in France.
    C. An email address titled info@business.com monitored by a specific individual.
    D. An identification number of a German candidate for a professional examination in Germany.

17. Under Article 17(1) (right to erasure or 'right to be forgotten'), what is a controller required to do when they receive a proper request for erasure from a data subject?

    A. Provide the data subject with a copy of the information that was deleted.
    B. Provide the requestor with a list of all of the recipients of their personal data.
    C. Immediately erase all the requesting data subject's personal data from backup files.
    D. Inform all third-party controllers processing shared personal data that they must delete it.

18. What is one major goal that the OECD Guidelines, Convention 108 and the Data Protection Directive (Directive 95/46/EC) had in common but largely failed to achieve in Europe?

    A. The restriction of cross-border data flows.
    B. The creation of legally binding data protection principles.
    C. The synchronisation of the approaches to data protection.
    D. The establishment of a list of legitimate data processing criteria.

19. An organisation wants to use a digital identity verification app to authenticate the identities of new customers. Customers will be asked to upload a photo ID document such as passport, driving licence or national ID and then asked to upload a picture of their face in the app. The ID document's authenticity is checked, and biometrics are used to ensure the ID document belongs to the customer.

    What step should the organisation take to ensure the data minimisation principle is implemented when collecting the personal data?

    A. Inform individuals in a privacy notice as to what information will be collected and how it will be used.
    B. Ask customers for consent to process the personal data for the purpose of verifying their identity.
    C. Undertake a data protection impact assessment to identify and assess the risk to individuals for this activity.
    D. Identify the legitimate interest for processing digital identification information and document this in an assessment.

20. Which of the following is **NOT** one of the seven EU-U.S. and Swiss-U.S. Privacy Shield Principles?

    A. Choice.
    B. Access.
    C. Security.
    D. Storage limitation.

21. When determining whether to impose an administrative fine and its amount, a supervisory authority takes into account the intentional or negligent character of the infringement. Which of the following is another criterion that would have a bearing on the amount of the fine?

    A. The actions the data controller takes to mitigate the damage suffered by data subjects.
    B. The type of industry in which the data controller conducts the core of its business activities.
    C. The data controller's insurance policy for security breaches and relevant coverage thresholds.
    D. The liability limitations in the commercial contract between the data controller and the data processor.

22. Under the GDPR, which of the following statements is **TRUE** regarding a data subject's right to opt out of direct marketing?

    A. The opt-out request can be expedited by charging a reasonable fee to the data subject.
    B. The right to opt out must be exercised within 30 days of the first communication with the data subject.
    C. The right to opt out excludes the retention of profiling data provided that all other personal data is deleted.
    D. The right to opt out applies to direct marketing sent in any way, including by post, phone and electronic mail.

23. Pursuant to Article 32(1) of the GDPR, which is a technical and organisational measure to ensure a level of security appropriate to the assessed risks?

    A. The anonymisation and sanitisation of personal data in such a way that the data subject is no longer identifiable.
    B. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
    C. The appointment of a DPO in charge of notifying regulators and data subjects about security incidents in a timely manner.
    D. The creation of a security incident management system to analyse incidents and threats in real time together with a complementary policy.

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

    A. Data that has been rendered unreadable to cast doubt on a data subject's identity.
    B. Data that has been stripped of personal identifiers to prevent a data subject's personal identity from being revealed.
    C. Data that has been replaced with random values to make it uniquely difficult to be tied back to a data subject's identity.
    D. Data that cannot be attributed to a specific data subject without the use of additional information kept separately.

25. Each of the following should be considered when assessing which security measures would be most appropriate for an organisation EXCEPT?

    A. The cost of implementing security measures.
    B. The sensitivity of the information to individuals.
    C. The lawful basis for processing the personal data.
    D. The potential harm caused if there was a personal data breach.

SCENARIO II
Please use the following scenario to answer the next FOUR questions.

You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong, and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is from international sales.

The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing due to the increased possibilities offered: The figures can answer children's questions on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.

When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers making it appear as though the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been

outsourced to a data centre located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.

In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a near-field communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.

26. Why is this company obligated to comply with the GDPR?

    A. The company has offices in the EU.
    B. The company employs staff in the EU.
    C. The company's data centre is in a country outside the EU.
    D. The company's products are marketed directly to EU customers.

27. To ensure GDPR compliance, what should be the company's position on the issue of consent?

    A. Parental consent for a child's use of the action figures would have to be obtained before any data could be collected.
    B. Consent for collecting the child’s personal data is implied through the parent's purchase of the action figure for the child.
    C. The child, as the user of the action figure, can provide consent himself, provided no information is shared for marketing purposes.
    D. Written authorisation attesting to the responsible use of children's data would need to be obtained from the supervisory authority.

28. What presents the biggest potential privacy issue with the company's practices?

    A. The NFC portal can read any personal data stored in the action figures.
    B. The cloud service provider is in a country that has not been deemed adequate.
    C. The information about the data processing involved has not been specified or updated.
    D. The RFID tag in the action figures has the potential for misuse because of the toy's evolving capabilities.

29. Considering the requirements of Article 32 of the GDPR (related to the security of processing), which practice should the company institute?

    A. Encrypt the data while it is in transit over the wireless Bluetooth connection.
    B. Include dual-factor authentication before each use by a child to ensure a minimum amount of security.
    C. Include three-factor authentication before each use by a child to ensure the best level of security possible.
    D. Insert contractual clauses into the contract between the toy manufacturer and the cloud service provider since South Africa is outside the European Union.

END OF SCENARIO II QUESTIONS

30. How has the GDPR's position on consent **most likely** affected app design and implementation?

    A. Users will see fewer advertisements when using apps.
    B. App developers' responsibilities as data controllers will increase.
    C. App developers will expand the types and amount of data necessary to collect for an app's functionality.
    D. Users will be presented with granular, specific consent requests for particular processing activities.

31. A convenience store in Brussels is having trouble with individuals spray painting graffiti on the front windows and entrance when the store is closed. As a security measure, they have installed video surveillance outside of their entrance. The camera records activity near the door and along the sidewalks in front of the store. Video footage is stored for one month and then deleted if not needed. Footage of a passer-by was captured while he was on the sidewalk and did not show evidence of vandalism by him. He asks to have his personal data erased immediately.

    What must the store do to comply with the GDPR?

    A. Ask the data subject to fill out a written request.
    B. Refuse to delete the data based on legitimate interest.
    C. Honour the request by erasing the data without undue delay.
    D. Accept the data subject’s oral request and respond within 90 days.

32. Before deciding to encrypt personal data, an organisation is required to assess the risks of the processing activity. What should an organisation take into consideration during the assessment?

    A. The sensitivity of the personal data to be processed, together with the data processor’s ability to maintain confidentiality and integrity of such data.
    B. The state of the art, the cost of implementation, and the nature, scope, context and purposes of processing, together with the impact on the data subject’s rights.
    C. The number of security incidents that resulted in personal data breaches and the associated number of reports submitted to data protection regulators for the previous fiscal year.
    D. The number of data subjects whose personal data is being collected, stored and processed and the location of the hosting servers, especially if the hosting servers are located in non-EEA countries.

33. Under the GDPR, who would be **least likely** to be allowed to engage in the collection, use and disclosure of a data subject's sensitive medical information without the data subject's knowledge or consent?

    A. A member of the judiciary involved in adjudicating a legal dispute involving the data subject and concerning the health of the data subject.
    B. A public authority responsible for public health, where the sharing of such information is considered necessary for the protection of the general populace.
    C. A health professional involved in the medical care for the data subject, where the data subject's life hinges on the timely dissemination of such information.
    D. A journalist writing an article relating to the medical condition in question, who believes that the publication of such information is in the public interest.

34. A shopping mall uses video surveillance cameras, which include facial recognition technology, at the entrance. This technology allows the mall to detect and remove individuals who were previously banned from the property.

    Which GDPR condition for processing would the shopping mall need to rely on for the processing of the video footage and facial recognition data?

    A. Explicit consent.
    B. Legitimate interest.
    C. Performance of a contract.
    D. Compliance with a legal obligation.

35. Each of the following are means controllers must use to meet fair processing information guidelines EXCEPT?

    A. Accessibility.
    B. Consistency.
    C. Conciseness.
    D. Transparency.

36. A key component of the OECD Guidelines is the 'individual participation principle'. What parts of the GDPR provide the closest equivalent to that principle?

    A. The lawful processing criteria stipulated by Articles 6 to 9.
    B. The rights granted to data subjects under Articles 12 to 23.
    C. The information requirements set out in Articles 13 and 14.
    D. The breach notification requirements specified in Articles 33 and 34.

37. A data controller must notify a data subject about a personal data breach likely to result in a high risk to the data subject's fundamental rights and freedoms in each of the following situations EXCEPT?

    A. When the data subject has opted out from receiving any type of future communications from the data controller.
    B. When the data breach was discovered 72 hours after its occurrence and has since become irrelevant to the data subject.
    C. When the data controller has already notified the data protection authority in the jurisdiction where the data breach took place.
    D. When the data controller has taken subsequent measures to ensure that the risks to the data subject are no longer likely to materialise.

38. A restaurant has a website through which customers order food to be delivered to their home. The restaurant sends the consumer's personal data and order information to a third-party delivery company for the purpose of delivering the food and accepting payment. After the order is complete, the delivery company pseudonymises the customer information to be used to improve the delivery company's estimated delivery time algorithm. The delivery company is not using the pseudonymised customer data for their algorithm on the restaurant's behalf.

    Under the GDPR, what role **best** describes the delivery company with respect to the processing of data used for the algorithm?

    A. Sub-processor.
    B. Joint controller.

C. Data controller.
D. Data processor.

SCENARIO III
Please use the following scenario to answer the next TWO questions.

The U.S.-based ABC Company is setting up a processing facility in Ireland. The company is a back-office data processor for EU health insurance companies. ABC Company's first client is Ireland HealthU Insurance, which provides health insurance for all college students in Ireland. The student health insurance applications include name, date of birth, and previous and existing medical treatments and conditions. The volume of data processing is unknown, but it is expected to be between 50,000–100,000 applications per month. Even though there are large volumes of applications, the number of employees of ABC Company remains fewer than 100.

39. Does the record-keeping requirement of the GDPR apply to this company?

A. No, because the company has fewer than 100 employees.
B. No, because the record-keeping requirement only applies to controllers.
C. Yes, because the company is processing special categories of EU personal data.
D. Yes, because any company processing EU personal data must adhere to the requirement.

40. In the above scenario, ABC Company appointed a DPO to comply with the GDPR. Why is ABC Company required to do so?

A. Their core activity involves processing EU sensitive data on a large scale.
B. All data controllers and processors operating in the EU must appoint a DPO.
C. Companies processing student personal data in the EU must appoint a DPO.
D. Any public company that is processing EU personal data must appoint a DPO.

END OF SCENARIO III QUESTIONS

41. Under the ePrivacy Directive, when obtaining consent from individuals to process their location data, controllers must present individuals with each of the following EXCEPT:

A. Details about the purposes and duration of the processing of location data.
B. Information about their right to withdraw consent of the processing at any time.
C. Information about the types of location data that will be collected and processed.
D. The details of any third parties where the location data will be transmitted.

42. A United States-based online company uses software to track the browsing behaviour and predict future purchases of its European customers. It also shares this information with third parties. Under the GDPR, what is the online company's primary obligation before engaging in this kind of profiling?

A. It must be able to demonstrate a prior business relationship with the customers.
B. It must solicit informed consent from the customers through a notice on its website.
C. It must prove that it uses sufficient security safeguards to protect customer data.
D. It must seek authorisation from the European supervisory authorities to track customers.

43. Which EU entity has the authority to invalidate adequacy determinations made by the European Commission?

    A. Council of the EU.
    B. Council of Europe.
    C. European Parliament.
    D. Court of Justice of the EU.

44. A company based in Spain is expanding its business to serve customers in other EU member states. The company increases its advertising budget and serves advertisements to market its product to consumers in France, Germany and the Netherlands. Consumers from all three countries use the company website to purchase products and have the products shipped to their homes. The privacy notice of the Spanish company provides data subjects with all the required information; however, the policy is only available in Spanish. Which GDPR principle is the company **most likely** to be in breach of?

    A. Integrity.
    B. Accuracy.
    C. Openness.
    D. Transparency.

45. What is the main reason GDPR Article 4(22) establishes the concept of the 'supervisory authority concerned'?

    A. To encourage the consistency of local data processing activity.
    B. To give corporations a choice about who their supervisory authority will be.
    C. To ensure that the interests of data subjects residing outside the lead authority's jurisdiction are represented.
    D. To ensure the GDPR covers controllers that do not have an establishment in the EU but have a representative in a member state.

46. Your company's chief information security officer is performing an annual review of its 'bring your own device' (BYOD) program for its European subsidiary. She has asked you to validate that the technical team's process document is compliant with GDPR. Which step would **result in non-compliance** with the GDPR?

    A. Implementing encryption at rest and in transit to protect personal data.
    B. Assuring basic security measures, such as device locking with password.
    C. Allowing access to all apps on the device to monitor for security risks or flaws.
    D. Controlling remote access by ensuring there are reasonable user authentication protocols.

47. Which of the following is **TRUE** with regard to the provisions of the ePrivacy Directive?

    A. They set forth the requirements for controllers to obtain consent solely for marketing through text messaging.
    B. They require websites to obtain user consent for all cookies, including those necessary for the site to function.
    C. They are more specific than the GDPR and therefore data controllers need only comply with the ePrivacy Directive.
    D. They do not constitute a binding law on data controllers but are requirements for EU member states to enact legislation.

48. A Brazilian citizen is visiting Paris, France on a one-year work visa. During their time in France, they join a local health and fitness club. The registration form for the health club requests their full name, permanent home address, bank account information for withdrawal of membership fees, and their race or ethnic origin for statistical purposes.

    Which information requested is considered a special category of personal data under Article 9 of the GDPR?

    A. Full name.
    B. Racial or ethnic origin.
    C. Bank account information.
    D. Permanent home address.

49. A bakery placed a video surveillance camera in the employee break room. The camera is pointed in a manner so that it only records the portion of the wall that holds the employee timeclock. The employer setup the camera after some employees were caught clocking in for other employees who were running late to work. The employer reviews the footage weekly and then deletes the footage. A sign is posted next to the timeclock informing employees about the recording.

    If the employees exercise their right to object, what will the employer need to do to continue the video monitoring?

    A. The employer must show compelling legitimate grounds that override the rights of the data subjects.
    B. The employer may continue as the recordings are on private property within the employee break room.
    C. The employer would have to cease video surveillance as the data subjects have withdrawn consent.
    D. The employer must show that the processing activity is not likely to result in a high risk to the rights and freedoms of individuals.

50. Under Article 21 of the GDPR, a controller must stop profiling when requested by a data subject unless the controller can demonstrate compelling legitimate grounds that override the interests of the individual. In the 'Guidelines on Automated individual decision-making and Profiling', the European Data Protection Board (EDPB) says the controller needs to do all of the following to demonstrate it has such legitimate grounds EXCEPT?

    A. Consider the importance of the profiling to the controller's particular objectives.
    B. Consider the impact of the profiling on the data subject's interest, rights and freedoms.
    C. Demonstrate that the profiling is for the purposes of direct marketing and in the controller's best interest.
    D. Carry out an exercise that balances the controller's interest and the basis for the data subject's objection.

51. Under which of the following conditions is a controller in the EU likely to be exempt from having to inform data subjects of the processing of their personal data under Articles 13 and 14 of the GDPR?

    A. If the controller purchases the personal data from a third-party seller.
    B. If the data subject is already aware of the processing of their personal data.
    C. If the data subject provided the personal information to another third party.
    D. If the data subject provided the personal data directly to the controller.

SCENARIO IV
Please use the following scenario to answer the next THREE questions.

Museum4yourSenses is a new museum with an exceptionally modern feel and is gaining a lot of traction on PluckPlack, a popular social media app. To promote their multi-location launch, founders aim to go viral with captivating avatar-enhanced videos on PluckPlack.

The museum's unique pitch is a chance for the first 100 visitors of the day to test out new virtual reality headsets for free. Visitors first step into a rainbow-colored waiting room where they receive instructions to speak their name and introduce the character they wish to become for the day. When visitors get their photo taken for their badge, they are instructed to look directly at the camera and make a funny face.

A month before the museum opened in Brussels, a private reception was held. The organisers gave visitors forms that included a box to acknowledge having read the museum's privacy notice and a consent form to sign about the images and voice recordings that would be required for entry. The consent form stated the personal data would be deleted 24 hours after the initial visit. After the Brussels launch, some of the visitors noticed the museum had posted promotional videos on PluckPlack that used the visitors' introductory voice recordings. The consent forms did not mention that the audio recordings would be combined with new avatars for the museum's reuse.

52. After visiting the Museum4yourSenses, what would visitors be entitled to request regarding their personal data?

    A. That the museum stop using their names and voices via social media channels.
    B. That the museum cease processing their personal data immediately upon receipt of their request.
    C. That a copy of the images and videos created from their introductions be provided for their own personal social media use.
    D. That monetary compensation be provided to them based on the number of views received by each video in which their likeness appears.

53. Bubbaloo Clown Company downloaded the PluckPlack videos promoting the museum and used the expressions to make new clown masks. It named the masks according to the visitor's introductions. When former visitors became aware of these masks, they lodged a series of complaints with the supervisory authorities. Museum4yourSenses deflected any responsibility, stating it was their audio-visual vendor handling the audio recordings of the visitors.

    Which statement about responsibility for the misuse of the visitors' personal data is correct?

    A. The audio-video vendor is responsible because they used the data in a way that wasn't consistent with their contract with Museum4yourSenses.
    B. As the controller, Museum4yourSenses is responsible for the audio-visual vendor's processing of personal data as provided in the contract between the museum and the vendor.
    C. The audio-visual vendor is not responsible because it has limited its liability in the Museum4yourSenses privacy notice that visitors acknowledged having read prior to entry.
    D. Museum4yourSenses is not responsible for the audio-visual aspects of the visit and limits their responsibility to the personal data related to the registration as indicated on the consent form.

54. A local elementary school teacher was one of the first visitors to Museum4yourSenses and was inspired to launch some educational materials after the visit. However, the teacher was alarmed to learn that a number of children with special needs had their introductory videos selected to promote a diversity and inclusion angle in the promotional materials. What would be her **best** option to protect children's rights?

    A. Send a registered letter to the museum requesting the museum deidentify the personal data to prevent processing personal data without a legal basis, especially of a vulnerable population and for commercial gain.
    B. Send a registered letter to the Museum4yourSenses board members, which includes a member of the EU Directorate General for Education, instructing them to immediately cease processing a vulnerable population's personal data.
    C. Submit a complaint with the supervisory authority requesting that Museum4yourSenses restrict processing, citing the large number of children and sensitive data elements that were being processed.
    D. Email the Museum4yourSenses administration alerting them to her concerns, citing the fact that children's personal data was being used without proper consent (of parents or authorised guardians) and therefore, the museum was relying on invalid consent to use this information and should immediately cease processing.

END OF SCENARIO IV QUESTIONS

55. A company is hesitating between binding corporate rules and standard contractual clauses as a global data transfer solution. Which of the following statements would help the company make an effective decision?

    A. Binding corporate rules are especially recommended for small and medium-sized companies.
    B. The data exporter does not need to be located in the EU for standard contractual clauses to be valid.
    C. Binding corporate rules provide a global solution for all the entities of a company that are bound by the intra-group agreement.
    D. The company will need the prior authorisation of all EU data protection authorities for concluding standard contractual clauses.

56. Which of the following is **NOT** a common service model of cloud computing?

    A. Platform as a Service (PaaS).
    B. Software as a Service (SaaS).
    C. Everything as a Service (EaaS).
    D. Infrastructure as a Service (IaaS).

57. You accidently send an email that contains a small amount of personal data, and no sensitive data, concerning 25 individuals from the EU to the wrong email address. You immediately request the recipient delete the email and the recipient confirms they have done so. After reporting what has happened to your DPO, you take some refresher privacy training for good measure.

    Under the GDPR, why is it unlikely that your company would be fined as a result of this data breach?

    A. There was no notification made to the DPA.
    B. There was no sensitive data involved in the breach.
    C. The company took all necessary steps to mitigate this breach.

D. There are no fines for breaches involving fewer than 50 individuals.

58. What is the core concept underpinning the GDPR accountability requirement?

A. The obligations with which an organisation must comply to demonstrate and show evidence of their compliance.
B. The internal allocation of privacy responsibilities to show appropriate assignments have been made.
C. The obligation for controllers to provide data subjects with information about the processing of their personal data.
D. The development of internal policies that outline how data should be processed and handled across the organisation.

59. What should an organisation consider when determining appropriate periods for retaining personal data?

A. Whether the stated purpose for collecting the personal data still applies.
B. Whether the personal data is stored on premise or with a cloud storage provider.
C. Whether the personal data can be retained for an undetermined future use.
D. Whether there was a lawful basis for processing when the personal data was collected.

60. When is a data sharing agreement **most likely** to be needed?

A. When personal data is being proactively shared by a controller to support a police investigation.
B. When personal data is being shared between commercial organisations acting as joint data controllers.
C. When anonymised data is being shared between a controller and a processor for analytical purposes.
D. When personal data is being shared with a public authority with powers to require the personal data to be disclosed.

61. Which treaty created the European Union?

A. 1951 Treaty Establishing the European Coal and Steel community.
B. 1957 Treaty Establishing the European Economic Community.
C. 1992 Maastricht Treaty.
D. 2007 Lisbon Treaty.

62. If a multi-national company wanted to conduct background checks on all current and potential European-based employees, what key provision would the company have to follow?

A. Background checks on European employees are regulated under the GDPR and employers must comply with the guidance therein.
B. Background checks on European employees can be performed only after receiving explicit consent from all employees based in Europe.
C. Background checks on European employees will be regulated by data protection and employment laws in the appropriate member state.
D. Background checks on European employees are not allowed, but the company can create a list of ineligible individuals based on its legitimate interests.

63. What is a 'layered fair processing notice'?

A. A notice that provides the data subject with information about the purposes of processing a specific item of personal data.
B. A notice that contains the controller's and processor's contact information and links to different topics within the notice.
C. A notice no longer than a certain number of words, listing key rights and using bullet points linked to more detailed information.
D. A notice wherein the key information is presented initially, and more detailed information is made available on a secondary page.

SCENARIO V
Please use the following scenario to answer the next THREE questions.

Excited to go on holiday, Isabelle took a trip to Amsterdam and went on a series of canal tours promoted by Novatours, a new Amsterdam-based company. She downloaded the Novatours app on her smartphone, accepted the privacy conditions, and connected her credit card for ease of payment. Upon return to her residence in France, she received frequent flyers from Novatours and third-party vendors. The number of flyers and vendors involved increased over time, including not only tourist activities, but also hotels, restaurants, car rentals, museum events, etc. All flyers mentioned a partnership with Novatours.

A few weeks later, she moved to a new apartment. She tried to contact Novatours but she could not get past the automated telephone system or the 'no-reply' general email on their website. Isabelle concluded there was no way to contact them other than through an affiliated tourist office where she first learned about the company.

64. Isabelle wants to update her address and limit the sharing of her personal data. What should she do?

A. Send a registered letter to the tourist information centre where she learned about Novatours, demanding her address be corrected and opting out of data sharing.
B. File a complaint with her local supervisory authority stating she cannot reach Novatours directly and ask them to demand that Novatours and its partners stop processing her personal data.
C. Send an email to the Dutch Tourist Authority via their website requesting they mandate Novatours to update her address and demand they stop sharing her address with other vendors.
D. File an official complaint with her local community's civil population division for protection of her private information and reference the file number in a demand letter to Novatours to restrict processing.

65. Finally, Isabelle received a response from Novatours about how she can delete her personal data from their records. She authenticated her identity via email and followed the instructions provided by Novatours to delete her data. But a few weeks later, she received text messages about new offers encouraging her to respond quickly before discounts expire. Isabelle suspects Novatours is still processing her personal data and wonders if this is allowed.

    Which of the following is correct?

    A. Novatours must stop processing Isabelle's personal data once a supervisory authority compels them to do so, without further authentication.
    B. Novatours can continue to process Isabelle's personal data if she fails the multi-factor authentication process.
    C. Novatours can continue to process Isabelle's personal data if she does not respond to identify verification requests within 30 days.
    D. Novatours must stop processing Isabelle's personal data once she has verified her identity and exercised her right to restrict processing.

66. Novatours received several similar complaints resulting in the suspension of their licence to operate. When Novatours' lawyer filed a complaint against the supervisory authorities, they were informed that Novatours, as a controller, was legally required to do which of the following?

    A. Respond within 30 days of receipt of the request.
    B. Provide contact details of the data protection officer.
    C. Provide an attestation with the date the personal data has been deleted.
    D. Honour all data subject requests cited with clear and compelling examples.

END OF SCENARIO V QUESTIONS

67. An unforeseen power outage results in Company Z's lack of access to customer data for six hours, which is considered a breach under Article 32 of the GDPR. Based on the WP29's February 2018 'Guidelines on Personal data breach notification' (later adopted by the EDPB), Company Z should do which of the following?

    A. Conduct a thorough audit of all security systems.
    B. Notify affected individuals that their data was unavailable.
    C. Notify the supervisory authority about the loss of availability.
    D. Document the loss of availability to demonstrate accountability.

68. Which instrument could be used, or which treaty could be joined, by a non-European country that wanted to demonstrate an international commitment to implement data protection legislation and to provide protection of individuals with regard to automatic processing of personal data?

    A. Directive 95/46/EC.
    B. The Treaty of Lisbon.
    C. The Council of Europe's Convention 108.
    D. Charter of Fundamental Rights of the European Union.

69. In what stages of the project life cycle should data protection by design (also known as privacy by design) be applied?

    A. During the entire project life cycle.
    B. After the development but prior to launch.
    C. Only during the initiation and planning stages.
    D. Continually after the project is productionised.

70. A data subject makes a subject access request (SAR) to an online retail company for their personal data. The data subject states that they are making a SAR in accordance with the GDPR; however, if the company credits the data subject's online account with a specified sum of money, the data subject will withdraw their request. The company has not had any previous access requests by other individuals.

    Which of the following would be legitimate grounds for the company to refuse to comply with the access request?

    A. The request is manifestly unfounded or excessive.
    B. The request is frivolous and will be time consuming.
    C. No other individual has made a similar request for access.
    D. The company has a policy in place rejecting all access requests.

71. Under the GDPR, which of the following is **TRUE** about data subjects' options to exercise their rights in cases of noncompliance?

    A. Individuals need to choose whether to take their complaints about noncompliance to DPAs or to the courts, as they cannot do both simultaneously.
    B. Individuals can only seek administrative or judicial remedies to noncompliance once they have made prior complaints to the controller or processor.
    C. Individuals can take their complaints to DPAs and/or to the courts, regardless of whether they made prior complaints to the controller or processor.
    D. Individuals can only take their complaints about noncompliance to the courts via class actions, whereby a group of individuals are represented as a collective before the courts.

72. Which statement about automated decision-making under Article 22 of the GDPR is **TRUE**?

    A. Automated decision-making that would otherwise be prohibited is allowed if it is authorised by law.
    B. Data subjects must notify controllers that they do not want to be subject to automated decision-making.
    C. The right to object to automated decision-making is triggered any time decisions are made by automated processes.
    D. Automated decision-making is permitted provided it is first reviewed by a person that cannot influence the outcome.

73. Under the ePrivacy Directive, when a company decides to send direct email marketing, which of the following legal bases may it generally rely on?

    A. Consent and legitimate interest.
    B. Consent and performance of a contract.
    C. Public interest and compliance with a legal obligation.
    D. Legitimate interest, consent and performance of a contract.

74. A data subject wants to lodge a complaint against a controller about the processing of their data. Which of the following is **NOT** a true statement?

    A. Data subjects are entitled to know about the risk of security breaches involving their personal data.
    B. Data subjects have broad rights of recovery and can even recover for nonmaterial damage and/or distress.
    C. Data subjects can lodge a complaint with a DPA or the courts without complaining to the applicable controller first.
    D. Where multiple parties are involved, any individual controller or processor involved is liable for the full amount of the damage.

75. A company is under investigation by multiple regulators in different countries' jurisdictions for not complying with GDPR fair notice requirements. Which is **TRUE** of the fines that may be assessed against the company?

    A. A company can only be fined by one member state even if it has breached the GDPR in several jurisdictions.
    B. The criteria of whether and to what extent fines may be imposed can vary depending on the member state, which would affect the total fines to be imposed.
    C. The combined fines for all violations cannot exceed €10 million or 2% of the total worldwide annual turnover of the preceding fiscal year.
    D. The criteria for what constitutes a breach of the GDPR is different in each member state, which would affect the total fines to be imposed.

76. An employee of company XYZ has just noticed a memory stick containing records of client data, including their names, addresses and full contact details, has disappeared. The data on the stick is unencrypted and in clear text. It is uncertain what has happened to the stick at this stage, but it likely was lost during the travel of an employee.

    What should the company do?

    A. Notify the data protection supervisory authority as soon as possible that a data breach may have taken place.
    B. Immediately notify all customers of the company that their information has been accessed by an unauthorised person.
    C. Launch an investigation and if nothing is found within one month, notify the data protection supervisory authority.
    D. Invoke the 'disproportionate effort' exception to postpone notifying data subjects until more information can be gathered.

SCENARIO VI
Please use the following scenario to answer the next TWO questions.

Luca is the owner of a chain of Italian restaurants across Europe. The restaurant has been successful but beginning with the COVID pandemic customers have mainly ordered food to pick up and eat at home. Luca decided to create a mobile app that allows customers to order ahead and schedule pickup times to help alleviate wait times. This also allowed him to build analytics to better staff his restaurants in this new era of takeout.

77. To comply with the obligations under Article 25 (data protection by design and by default), what should Luca consider when reviewing and assessing the processing and storage of personal data gathered by his app?

A. How many customers will use the application during a specific time frame.
B. How the data can be used to create advertisements for further monetisation.
C. How to create a shared responsibility matrix so all staff members are aware of privacy requirements.
D. What is the least amount of personal data necessary to run the app and provide the scheduled pickup time.

78. Since Luca is now processing and storing customer data via his app, he needs to create internal privacy policies for employees to follow. Which guidelines should be included in the policy?

A. Scope, individual rights and employee responsibilities.
B. Policy statement, policy compliance and transparency.
C. Scope, reporting incidents and employee responsibilities.
D. Policy statement, policy compliance and individual rights.

END OF SCENARIO VI QUESTIONS

79. Which of the following is a legally binding instrument?

A. The UN Universal Declaration of Human Rights.
B. The Asian-Pacific Economic Cooperation (APEC) Privacy Framework.
C. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ('OECD Guidelines').
D. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108').

80. A U.S.-based pharmaceutical company, Pharma, receives pseudonymised patient information from clinical sites all over the world, including the EU, as part of a clinical trial. How must Pharma process the data?

A. Pharma must de-pseudonymise all data they receive before it can be processed under any jurisdiction.
B. Pharma can process the data as is because it is part of a clinical trial and will be processed only in the U.S.
C. Pharma must comply with all applicable privacy laws based on the country where the data subject resides.
D. Pharma need only comply with the privacy laws concerning data processing that are in effect in the U.S. and the GDPR.

81. Which treaty was issued as a result of the enlargement of the European Community and the corresponding need to improve the efficiency and speed of decision-making processes?

A. The Treaty of Ghent.
B. The Treaty of Lisbon.
C. The Treaty of Lepanto.
D. The Treaty of the Hague.

82. When a situation arises in which neither an adequacy decision nor appropriate safeguards are in place, the GDPR sets forth specific derogations to allow data transfers. Which of the following is a requirement to transfer data under the derogations?

    A. The transfer is done after suitable safeguards are in place.
    B. The transfer concerns an unlimited number of data subjects.
    C. The transfer is necessary for the purpose of direct marketing.
    D. The transfer is done under the guidance of a data protection officer.

83. In which of the following situations must a data protection impact assessment (DPIA) be used?

    A. A clothing store wants to build aggregated metrics on the types of clothing their customers purchase by season.
    B. A start-up company specialising in online gaming is using new technologies to build a new battleship game.
    C. A bank is implementing surveillance cameras outside each of their buildings to help them identify possible bank thieves.
    D. A pool company is implementing a new advertising campaign targeted to customers who have visited their store in the past 12 months.

84. Which of the following processing conditions would prohibit an organisation from retaining personal data collected for conducting a webinar once the webinar has concluded and the processing purpose has expired?

    A. The data will be processed solely for archiving purposes in the public interest.
    B. The data will be processed for historical research or statistical purposes.
    C. The data is anonymised and then used for a participant demographics database.
    D. The data is processed to maintain a CRM database of webinar attendees.

85. A grocery store opened on a street that has had regular problems with thefts. Since the grocery store is new, they do not yet have the budget for a real surveillance system. Instead, they install fake video surveillance cameras to stop potential thieves until they can afford a real surveillance system. The cameras are pointed only inside the store and there are no cameras facing the street.

    Which GDPR lawful basis is the grocery store **most likely** to have relied on for the placing of the cameras?

    A. Consent.
    B. Legitimate interest.
    C. The GDPR does not apply.
    D. Performance of a contract.

86. Under what circumstances would the GDPR apply to personal data that exists in physical form, such as information contained in notebooks or hard copy files?

    A. Only where the personal data is handled in a sufficiently structured manner to form part of a filing system.
    B. Only where the personal data is treated by automated means in some way, such as computerised sorting, distributing or filing.
    C. Only where the personal data is subjected to specific computerised processing, such as image scanning or optical character recognition.

D. Only where the personal data is produced as a physical output of specific automated processing activities, such as printing, labelling or stamping.

87. The European Commission has the power to determine whether a country outside of the EU provides an adequate level of data protection in accordance with the GDPR. Which one of the following countries has been deemed 'adequate'?

A. Mexico.
B. Nigeria.
C. Uruguay.
D. Malaysia.

88. Failure to provide fair information to data subjects with regards to the processing of their personal data is **likely** to?

A. Require the processor to obtain a new authorisation to process the data subject's data.
B. Render the data unusable and require the processor to indefinitely suspend the processing of the data.
C. Require the processor to notify the data subject that their personal data has been permanently deleted.
D. Render the processing unfair, as well as constitute a violation of the Regulation's information provision obligations.

89. The GDPR requires parent/guardian consent to process personal data of data subjects younger than what minimum age?

A. 14.
B. 16.
C. 18.
D. 21.

90. Which of the following is the **best** approach for an organisation to take to be able to demonstrate fairness when processing personal data?

A. Providing a privacy notice to inform data subjects of how their personal data is going to be processed.
B. Implementing a privacy management framework to describe how the organisation manages privacy risk.
C. Implementing a privacy training plan to ensure all employees receive appropriate training suitable for their role.
D. Following a privacy-by-design approach to ensure that privacy is considered throughout the information life cycle.

Answer Key

For each correct response, place a "1" or a checkmark in the corresponding domain column. Note: the domain is indicated by an unshaded (white) box. Subdomains are noted in the blue columns.

Item Number	**Correct Answer**	**Domain I** Introduction to European Data Protection	*Domain I Sub Domain*	**Domain II** European Data Protection Law and Regulation	*Domain II Sub Domain*	**Domain III** Compliance with European Data Protection Law and Regulation	*Domain III Sub Domain*
1	**B**				*A*		
2	**C**				*G*		
3	**D**						*C*
4	**B**				*I*		
5	**B**		*B*				
6	**C**				*J*		
7	**B**				*B*		
8	**A**				*I*		
9	**C**		*C*				
10	**B**				*D*		
11	**D**				*K*		
12	**C**				*F*		
13	**B**						*A*
14	**C**						*A*
15	**B**						*A*
16	**C**				*A*		
17	**D**				*F*		
18	**C**		*A*				
19	**C**				*C*		
20	**D**				*I*		
21	**A**				*K*		
22	**D**						*C*
23	**B**				*G*		
24	**D**				*A*		
25	**C**				*C*		
26	**D**				*B*		
27	**A**				*E*		
28	**C**				*E*		
29	**A**				*G*		
30	**D**						*D*
31	**C**				*F*		
32	**B**				*G*		
33	**D**				*D*		
34	**A**						*B*
35	**B**				*E*		

Item Number	Correct Answer	**Domain I** Introduction to European Data Protection	*Domain I Sub Domain*	**Domain II** European Data Protection Law and Regulation	*Domain II Sub Domain*	**Domain III** Compliance with European Data Protection Law and Regulation	*Domain III Sub Domain*
36	**B**		*A*				
37	**D**				*G*		
38	**C**				*A*		
39	**C**				*H*		
40	**A**				*H*		
41	**D**				*C*		
42	**B**				*F*		
43	**D**		*C*				
44	**D**				*E*		
45	**C**				*J*		
46	**C**						*A*
47	**D**		*C*				
48	**B**				*A*		
49	**A**						*B*
50	**C**				*F*		
51	**B**				*C*		
52	**A**				*F*		
53	**B**				*A*		
54	**C**				*D*		
55	**C**				*I*		
56	**C**						*D*
57	**C**				*J*		
58	**A**				*H*		
59	**A**				*C*		
60	**B**				*G*		
61	**C**		*C*				
62	**C**						*A*
63	**D**				*E*		
64	**B**				*F*		
65	**D**				*F*		
66	**A**				*F*		
67	**D**				*H*		
68	**C**		*C*				
69	**A**				*H*		
70	**A**				*F*		
71	**C**				*K*		
72	**A**				*F*		
73	**A**				*C*		
74	**A**				*K*		
75	**B**				*J*		

Item Number	Correct Answer	**Domain I** Introduction to European Data Protection	*Domain I Sub Domain*	**Domain II** European Data Protection Law and Regulation	*Domain II Sub Domain*	**Domain III** Compliance with European Data Protection Law and Regulation	*Domain III Sub Domain*
76	**A**				*G*		
77	**D**				*H*		
78	**C**				*H*		
79	**D**		*C*				
80	**C**				*B*		
81	**B**		*B*				
82	**A**				*I*		
83	**C**				*H*		
84	**D**				*C*		
85	**C**						*B*
86	**A**				*B*		
87	**C**				*I*		
88	**D**				*E*		
89	**B**				*D*		
90	**A**				*C*		
SUMMARY		**___ of 10 correct**		**___ of 68 correct**		**___ of 12 correct**	
PERCENTAGE (# correct/# total) x 100							

Item Rationales

1. The correct answer is B. Processing is defined by the Regulation as 'any operation or set of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. See Article 4(2) of the GDPR.
   Body of Knowledge Domain II, Subdomain A

2. The correct answer is C. A data breach occurs when the data for which an organisation is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity. If that occurs, and it is likely that the breach poses a risk to an individual's rights and freedoms, the organisation must notify the supervisory authority without undue delay and at the latest within 72 hours after becoming aware of the breach. If the organisation is a data processor, it must notify the data controller of any data breach without undue delay after becoming aware of it. If the data breach poses a high risk to those affected, then the controller should inform the data subjects unless there are effective technical and organisational protection measures that have been put in place or other measures that ensure the risk is no longer likely to materialise. As an organisation, it is vital to implement appropriate technical and organisational measures to avoid possible data breaches. See Article 33(2) of the GDPR.
   Body of Knowledge Domain II, Subdomain G

3. The correct answer is D. Under the GDPR, an organisation must disclose to data subjects how their personal data will be used and must obtain unambiguous consent for direct marketing unless the direct marketing falls and can be justified under the basis of legitimate interest. However, the organisation is not required to make specific direct disclosures about the lawful basis for processing to data subjects. The organisation would generally need to include information about its lawful basis)or bases, if more than one applies) in its privacy notice. In addition, organisations must disclose to consumers the actual names of any third parties with whom the data will be shared; providing the categories under which those third parties are classified is not sufficient. Encryption must be considered but is not required under the GDPR although it is a best practice for cybersecurity.
   Body of Knowledge Domain III, Subdomain C

4. The correct answer is B. Article 47 of the GDPR specifically references BCRs as legally binding data transfer mechanisms. It sets forth data subjects' enforceable rights as well as the elements that must be included. In addition to the three elements listed within the options are the details of the data transfers; the legally binding nature, both internally and externally, of the BCR; the acceptance for liability for any breaches of the BCR; the tasks of the data protection officer, if any; and how the BCR is communicated to the data subject.
   Body of Knowledge Domain II, Subdomain I

5. The correct answer is B. The ECHR is not an institution of the EU; instead, it is part of the apparatus of the Council of Europe, a broader group of member states than the EU. The ECHR was founded in 1959

to oversee the European Convention on Human Rights. Thus, it enforces the European Convention on Human Rights rather than EU law.

While the ECHR's powers don't encompass the implementation of EU law, the CJEU can force national governments to administer and honour EU law. The CJEU interprets EU law to make sure it is applied in the same way in all EU countries and settles legal disputes between national governments and EU institutions. It can also, in certain circumstances, be used by individuals, companies or organisations to take action against an EU institution if they feel it has somehow infringed their rights.
Body of Knowledge Domain I, Subdomain B

6. The correct answer is C. A lead supervisory authority (LSA) is assigned when a company operates in multiple EU jurisdictions. Article 56 requires, without prejudice to Article 55, that the supervisory authority of the main establishment or of the single establishment of the controller or processor be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60. Additionally, Article 60(1) creates duties of cooperation for cross-border processing. While the LSA is concerned with data subject rights, data access disputes and special categories of data, the lead role was established specifically for dealing with cross-border issues.
Body of Knowledge Domain II, Subdomain J

7. The correct answer is B. Whereas many of the requirements listed above could potentially trigger the extraterritorial effect of the GDPR, the processing of EU residents' personal data by a non-EU business that targets data subjects in the EU will always do so. If a non-EU company explicitly targets EU customers, then it is subject to GDPR compliance.
Body of Knowledge Domain II, Subdomain B

8. The correct answer is A. While industry standards and certifications of adherence to them are useful in demonstrating compliance capabilities, they would first need to be approved by the EU Commission to be considered a valid transfer mechanism. As of November 2021, the EU Cloud Code of Conduct, based on ISO standards, is the only approved code/certification under the GDPR.
Body of Knowledge Domain II, Subdomain I

9. The correct answer is C. The right to self-determination is an important right in democratic societies. It allows people to freely determine their political status and pursue economic, social and cultural development. However, it is *not* a right explicitly called out in the GDPR.

   The right to a fair trial, freedom of expression and freedom to conduct a lawful business are rights mentioned in Recital 4 of the GDPR.
   Body of Knowledge Domain I, Subdomain C

10. The correct answer is B. While it might seem reasonable to obtain explicit consent, consent would not apply here since providing fingerprints for access is required by the bank and is non-negotiable. (EDPB Guidelines 05/2020). Therefore, proving legitimate interest would be the bank's only legal basis: the legitimate interest being that it is necessary to provide the appropriate level of security the members

expect of the bank and that the processing relates solely to the members. Meeting one of the ten conditions for processing special categories of data under Article 9(2) would also be necessary. Under the GDPR, biometric data, such as fingerprints, is a special category of personal data. Biometric data is unique to each person and cannot be changed at will. It is therefore important to protect this type of data properly.
Body of Knowledge Domain II, Subdomain D

11. The correct answer is D. According to the GDPR, Art. 83, 'Each supervisory authority (SA) shall ensure that the imposition of administrative fines pursuant to this Article due to infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate, and dissuasive'.

    Supervisory authorities can levy significant fines against entities for GDPR violations which vary depending on the nature of the violation. However, before imposing a fine, the SA must consider a variety of factors (Article 83(2)). A proposed fine can be challenged in court and attempts to impose exorbitant fines have been rejected by the courts.
    Body of Knowledge Domain II, Subdomain K

12. The correct answer is C. The right to data portability did not exist in the Data Protection Directive; portability was one of the notable new inclusions in the GDPR. The Directive did allow for some right of access, although the GDPR expanded the categories of data that could be requested. The scope of the right to rectification was included in the Directive and was largely unchanged by the GDPR. Similarly, the Directive already allowed data subjects to restrict processing by requesting that certain data be 'blocked'.
    Body of Knowledge Domain II, Subdomain F

13. The correct answer is B. Since Building Block is considered a data controller, most of the responsibilities for compliance with GDPR falls to the data controller. The data controller is responsible for providing information to the data subjects, ensuring that processing has a legitimate basis and that the data subject's rights are honoured, carrying out data protection impact assessments in the case of high-risk processing, ensuring that there is appropriate security for data, and determining whether notification to data protection authorities (DPAs) or data subjects is necessary in case of a personal data breach.
    Body of Knowledge Domain III, Subdomain A

14. The correct answer is C. As required by the notice requirement under the Regulation, employers must provide employees with sufficient information about the monitoring activity. This transparency is important not only to meet the notice requirement but also to set employees' expectations about how their time at work will be monitored. Setting expectations is central to ensuring that monitoring is lawful.

    If employees have not been told that their behaviour will be monitored in the workplace, they have a greater expectation of privacy. Informing employees of how they will be monitored can reduce that expectation. It is not, however, possible for an employer to argue that a lack of privacy in the

workplace is acceptable just because the employer has warned employees that they have no workplace privacy. A court or DPA would not recognise such a comprehensive warning as legitimate since the law recognises that workers enjoy a certain degree of privacy in the workplace that cannot be completely eradicated.
Body of Knowledge Domain III, Subdomain A

15. The correct answer is B. The European Data Protection Supervisor issued 'Guidelines on personal data and electronic communications in the EU institutions' in December 2015, which align with guidance in the Regulation and in the ePrivacy Directive. Amongst other information to be provided to employees, companies should inform them of their rights, including whom to contact and how to do so, in the event of questions or concerns.
Body of Knowledge Domain III, Subdomain A

16. The correct answer is C. 'Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. A general email address for a business would not be considered personal data as it does not relate to and cannot be used to identify an individual.
Body of Knowledge Domain II, Subdomain A

17. The correct answer is D. According to GDPR Article 17(1), when a data subject submits a proper request that their personal data be erased, the controller must not only delete that data, where specific grounds apply, but when the controller has made the data public, it must inform third parties who are processing the published personal data as controllers that the data subject has exercised their right to erasure. A list of additional controllers does not need to be provided to the data subject under Article 17 as part of the controller's requirements to meet the erasure request; however, Article 13 does set forth requirements for disclosure of shared data.

    Backup data need not be deleted immediately; however, the controller must ensure that access to restoring the data is limited and can only be done once there has been a thorough review to ensure there has been no deletion request. There is no requirement for providing a copy of all deleted information.
    Body of Knowledge Domain II, Subdomain F

18. The correct answer is C. The OECD Guidelines, Convention 108 and the Data Protection Directive all had the goal of a synchronised approach to data protection, but it wasn't until the GDPR that the harmonised approach that each of them failed to achieve was realised. The OECD created a non-binding series of guidelines that served as the basis for many future laws. Convention 108, a Council of Europe treaty, stemmed partly from the OECD and was available for countries to utilise starting in 1981. In 1995, the European Union passed the Data Protection Directive (Directive 95/46/EC) which was Europe's primary data protection law until the GDPR went into effect on 25 May 2018.

A directive, unlike a regulation such as the GDPR, requires member states to enact their own legislation that serves as a country's version of that directive. One goal with the GDPR was to move to a regulation, which was a single law that applied automatically to the member states, creating a more synchronised and harmonised approach to data protection.
Body of Knowledge Domain I, Subdomain A

19. The correct answer is C. Processing biometric data for the purpose of identification is high-risk processing under the GDPR, so a data protection impact assessment is likely to be required for this activity. The assessment should consider whether this processing activity is necessary and whether the information collected is necessary to meet the purpose of identity verification and consider the minimum amount of information required to fulfil the purpose identified. The data minimisation principle states that personal data shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.
Body of Knowledge Domain II, Subdomain C

20. The correct answer is D. The seven Privacy Shield Principles are (1) notice; (2) choice; (3) security; (4) access; (5) accountability for onward transfer; (6) data integrity and purpose limitation; and (7) recourse, enforcement and liability. Once an organisation publicly commits to comply with the Privacy Shield Principles, that commitment is enforceable by the U.S. Federal Trade Commission under the authority of Section 5 of the FTC Act (prohibition on deceptive acts).
Body of Knowledge Domain II, Subdomain I

21. The correct answer is A. Article 83(2) of the GDPR provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and the amount of the fine. One of the criteria when determining whether to impose an administrative fine is any action taken by the controller or processor to mitigate the damage suffered by data subjects. See Art. 83(2) of the GDPR and WP29 'Guidelines (253/2017) on the application and setting of administrative fines for the purposes of the Regulation 2016/679'.
Body of Knowledge Domain II, Subdomain K

22. The correct answer is D. Under the GDPR, the right to opt out applies to all direct marketing formats. Data subjects have the right to opt out at any time. No fee may be charged to a data subject exercising the right to opt out.
Body of Knowledge Domain III, Subdomain C

23. The correct answer is B. The GDPR stipulates the following possibilities to ensure the security of personal data with an adequate level of protection: (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; or (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

According to the GDPR, the principles of data protection continue to apply to pseudonymised and encrypted data but do not apply to anonymised data since the latter no longer relates to an identified or identifiable individual.

Therefore, while data pseudonymisation and data encryption are security-enhancing technologies for the protection of personal data stored in databases, data anonymisation is a type of data sanitisation by which personal data are cleansed from databases to the point that the GDPR is no longer applicable. See Article 32(1) of the GDPR.
Body of Knowledge Domain II, Subdomain G

24. The correct answer is D. The GDPR defines pseudonymisation as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person. Pseudonymous data would include profiles that can be connected to an individual even where the controller does not, in fact, intend to make this connection. Pseudonymous data shall not be considered anonymous.
Body of Knowledge Domain II, Subdomain A

25. The correct answer is C. Article 5(1)(f) of the Regulation states that personal data must be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")'. To determine what is appropriate, an organisation will need to conduct a risk assessment. The assessment should consider the nature of the data being processed, potential threats and vulnerabilities to the data subject (such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed) and the cost of implementation (cost should be appropriate for the risks identified). The lawful basis for processing the personal data is unlikely to impact the integrity and confidentiality of the information being processed.
Body of Knowledge Domain II, Subdomain C

26. The correct answer is D. This is a non-EU company (1) explicitly targeting EU customers and (2) collecting data from persons in the EU. The GDPR aims to protect the privacy rights of all persons in the EU as well as the rights of any individuals who have their data processed by a company in the EU. As a result, non-EU companies explicitly targeting EU customers and therefore collecting the data of persons in the EU (such as the company in this scenario) must comply with the GDPR.
Body of Knowledge Domain II, Subdomain B

27. The correct answer is A. Under Article 8, where a controller relies on consent as the legitimate processing criterion and information society services are offered directly to a child, the processing of personal data is only lawful where the child is at least 16 years old. Where the child is under 16 years old, such processing is only lawful 'if and to the extent that consent is given or authorised by the holder of personal responsibility over the child. Member states may set a minimum age of consent less than 16 years so long as the age is not lower than 13'.
Body of Knowledge Domain II, Subdomain E

28. The correct answer is C. The toy manufacturer's privacy information does not clearly explain the processing that is taking place, resulting in a lack of transparency. This lack of transparency means that data subjects will not understand how and why their personal data is processed and will not be able to make an informed decision and may not be able to exercise their rights.
Body of Knowledge Domain II, Subdomain E

29. The correct answer is A. A key principle of the GDPR is the security principle which requires personal data be processed securely by means of appropriate technical and organisational measures. To put the appropriate technical and organisational measures in place, a risk analysis needs to be conducted and organisational policies, together with physical and technical measures, need to be applied. The state of the art and costs of implementation are to be considered when deciding what measures to take, but they must be appropriate both to the circumstances and the risk the processing poses. Where appropriate, measures such as pseudonymisation and encryption are required. These measures must ensure the confidentiality, integrity and availability of the systems and services and the personal data being processed within them. These measures must also include the ability to restore access and availability to personal data in a timely manner in the event of a physical or technical incident. Companies are required to have appropriate processes in place to test the effectiveness of these measures and undertake any required improvements. In this question, we have a toy that collects data from a child and transmits it via Bluetooth to another device. Transmission of this data should be protected from people or devices trying to intercept the communication between devices. One way to mitigate this concern is to encrypt the data in transit over the wireless Bluetooth connection. See GDPR Article 32(1)(a).
Body of Knowledge Domain II, Subdomain G

30. The correct answer is D. If consent is relied upon as the legal basis for processing, it must be specific, fully informed, freely given and revocable at any time (see GDPR Article 7). Because 'the request for consent shall be presented in a manner which is clearly distinguishable from other matters', granular and specific consent is required for each optional processing activity.
Body of Knowledge Domain III, Subdomain D

31. The correct answer is C. Because the footage in question no longer meets the purpose for which it was initially stored (i.e., no vandalism occurred during the time the data subject passed by), there is, at the time of the request, no legitimate interest to store the data that would override the interests of the data subject. The controller must honour the request and erase the personal data without undue delay pursuant to GDPR Article 17.
Body of Knowledge Domain II, Subdomain F

32. The correct answer is B. Companies can reduce the probability of a data breach if they choose to encrypt personal data. The processing of personal data is naturally associated with a certain degree of risk. Therefore, risk management plays an ever-larger role in IT security, and data encryption is suited, amongst other means, for these companies. In general, encryption refers to the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct decryption key. This minimises the risk of an incident during data processing, as encrypted contents are basically unreadable for third parties who do not have the

correct key. Encryption is the best way to protect data during transfer and one way to secure stored personal data. It also reduces the risk of abuse within a company, as access is limited only to authorised people with the right key. The GDPR also recognises these risks when processing personal data and places the responsibility on the controller and the processor to implement appropriate technical and organisational measures to secure personal data. The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case in order to accommodate individual factors. However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state of the art, implementation costs, and the nature, scope, context and purposes of the processing. See Recital 83 and Article 32 of the GDPR.
Body of Knowledge Domain II, Subdomain G

33. The correct answer is D. To be able to process health information, which is special category of data, the controller will need to have both a lawful basis under Article 6 and meet at least one condition under Article 9. Some of the conditions under Article 9 include where courts are acting in their judicial capacity, where it is necessary for reasons of public interest in the area of public health, and where processing is necessary to protect the vital interest of the data subject. For a journalist writing an article, processing is only permitted for reasons of substantial public interest where there is a basis in member state law.
Body of Knowledge Domain II, Subdomain D

34. The correct answer is A. In this situation, the personal data being collected is biometric data under GDPR Article 9. Biometric data is defined in GDPR Article 4(14) as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'. Video footage on its own is not necessarily biometric data unless it results from specific technical processing relating to physical, physiological or behavioural characteristics, which allow unique identification of the individual. In this case, we are told the facial recognition data is used specifically to identify previously banned patrons who are entering the mall. The processing of biometric data requires both a lawful basis and a condition for processing; otherwise, it is generally prohibited by GDPR Article 9(1), unless an exception in GDPR Article 9(2) applies. Of the answer choices, only explicit consent is listed as a condition for processing sensitive personal data under GDPR Article (9)(2)(a).
Body of Knowledge Domain III, Subdomain B

35. The correct answer is B. While consistency is important, it is not listed as part of the fair processing information guidelines.

    When providing information to data subjects with respect to the processing of the data subject's personal data, controllers should ensure that such information is:

    - Concise: Although there is a clear conflict between this requirement and the volume of fair processing information the Regulation mandates, controllers can assist data subjects by separating content into headed sections, using short sentences and paragraphs, and adopting a layered approach to information provision.

- Transparent: Controllers should be genuine, open and honest with data subjects, and not misleading. Data subjects should not be surprised by processing and, where there are risks or important consequences associated with it, these should be spelled out.
- Easily accessible: It should be clear where fair processing information is and how it can be accessed. Data subjects should not be required to search for it, including amongst other content, and the provision of information should be appropriate for the context in which personal data is obtained.

Two additional requirements are that the information be:

- Intelligible and in clear and plain language: The language used should be easy for the target audience to understand, and controllers should avoid overly legal language, jargon and terminology.
- Accurate and up to date: Fair processing information should therefore be regularly reviewed.

Body of Knowledge Domain II, Subdomain E

36. The correct answer is B. The individual participation principle of the OECD Guidelines refers to the right of the individual to obtain information about themselves from the data controller and to have that communication provided to them within a reasonable time, without excessive charge, in a reasonable manner, and in a form intelligible to them.

    The rights granted to data subjects under Articles 12 to 23 refer to articles of the GDPR that provide rights to the data subject. These rights align with those mentioned in the OECD principle, such as the right of access by the data subject.
    Body of Knowledge Domain I, Subdomain A

37. The correct answer is D. Article 34(3) of the GDPR states three conditions that, if met, do not require notification to individuals in the event of a breach: (1) The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption or by tokenisation. (2) Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and acted against the individual who has accessed personal data before they were able to do anything with it. Due attention still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned. (3) It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. See Article 34(3) of the GDPR and WP29 'Guidelines on Personal data breach notification under Regulation 2016/679' (WP250 rev.01).
    Body of Knowledge Domain II, Subdomain G

38. The correct answer is C. A company can have multiple roles, depending on a specific processing activity. A company can be a data controller for some processing activities and a processor for others. In this scenario, the delivery company's primary business is as a data processor, because they process data only at the instructions of the data controller (the restaurant) for the purpose of delivering orders.

However, this question asks specifically about the role of the delivery company with respect to the processing of data used for the algorithm. As to that specific processing activity, the delivery company has gone outside the scope of processing directed by the controller and has redefined the purpose and means of processing that data, thereby making them a data controller for this activity.

This scenario is further described by the European Data Protection Board's 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', adopted 7 July 2021.
Body of Knowledge Domain II, Subdomain A

39. The correct answer is C. Article 30's record-keeping requirement has an exception for companies that employ fewer than 250 people. However, the under 250 employee exemption does not apply if (1) processing is likely to result in a risk to the rights and freedoms of the data subjects; (2) processing is frequent and not occasional; or (3) processing involves special categories of data including biometrics, health data, genetic data or data related to a person's sex life or sexual orientation (also known as sensitive personal data). Health data processed by this data processor is considered sensitive personal data, and there will be frequent processing of the data (not occasional). This means the company cannot rely on the exception and must comply with the Article 30 requirement.
Body of Knowledge Domain II, Subdomain H

40. The correct answer is A. A company must appoint a DPO, whether it is a controller or a processor, if its core activities involve the processing of sensitive data on a large scale. 'Large scale' is defined as the number of data subjects concerned as a specific number or as proportion of the relevant population. Here, ABC Company will be processing all student health insurance applications in Ireland, which represents a large portion of the population.
Body of Knowledge Domain II, Subdomain H

41. The correct answer is D. Under Article 9(1) of the ePrivacy Directive, the requirement is to inform users or subscribers prior to obtaining their consent whether the data will be transmitted to a third party. The directive does not require details of any third party to be included.
Body of Knowledge Domain II, Subdomain C

42. The correct answer is B. The United States-based company is processing the personal data of European citizens and therefore must comply with the GDPR. Obtaining informed consent provides the strongest legal basis for processing personal data in this scenario. Informed consent may be in the form of a privacy notice that specifies the rights of the individual related to using personal data only for stated purposes, as well as informing data subjects of their ability to withdraw consent at any time. The notice must inform the website visitor about the software used, including automated decision-making systems, profiling and sharing personal data with other recipients. The privacy notice must include the contact details of the company, its EU representative and its data protection officer.
Body of Knowledge Domain II, Subdomain F

43. The correct answer is D. The Court of Justice of the European Union (CJEU) interprets EU law to make certain it is applied in the same way across all member states and settles legal disputes between national governments and EU institutions. It can also, in certain circumstances, be used by individuals,

companies or organisations to take action against an EU institution, if they feel it has somehow infringed their rights.
Body of Knowledge Domain I, Subdomain C

44. The correct answer is D. This GDPR principle is first mentioned in Article 5(1)(a) as personal data that must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'. This question is primarily related to transparency. Transparency is mentioned again in GDPR Article 14(1) and requires the controller to provide data subjects with information about the data processing 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'.
In this question, a Spanish company is knowingly engaged in the sale of products to consumers in countries where the primary language is not Spanish. Since the company is advertising to data subjects in non-Spanish speaking countries, they have an obligation to provide those data subjects with transparency around their processing activities in a language that is readable to them.
Body of Knowledge Domain II, Subdomain E

45. The correct answer is C. For companies that process data outside of their lead supervisory authority's location, the concept of 'supervisory authority concerned' gives the DPA the ability to also represent the interests of individuals residing outside of the lead authority's jurisdiction. For example, where there is a regulatory problem that concerns a controller in one jurisdiction and a processor in another jurisdiction, the lead authority will be the controller's while the processor's authority will be a 'supervisory authority concerned'. As noted in Article 56(2), 'By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State'. (Reference section 13.5.2 in *European Data Protection, Second Edition*).
Body of Knowledge Domain II, Subdomain J

46. The correct answer is C. Many companies allow for their employees to use personal devices for communications in the workplace ('bring your own device' or BYOD). Since allowing BYOD may raise a number of potential privacy issues, it is of utmost importance that the company put together a BYOD program in view of the GDPR provisions. Companies are required to respect the privacy of employees who use personal equipment in the context of their professional activity and should compartmentalise the areas of the device intended to be used in a professional context (e.g., create a security bubble) to ensure personal information cannot be accessed. Additionally, the company must ensure the user understands the risks of using their own device, including precautions to keep data safe.
Body of Knowledge Domain III, Subdomain A

47. The correct answer is D. The ePrivacy Directive is not a binding law. It sets forth guidance for the EU member states to create laws within their borders to achieve the specific requirements set forth in the Directive. The Directive regulates electronic communications including, but not limited to, cookie usage and digital marketing including phone, fax, email and text messages. While the Directive includes many privacy aspects, including data minimisation and consent requirements, it does not focus solely on personal data, which is the purview of the GDPR.
Body of Knowledge Domain I, Subdomain C

48. The correct answer is B. GDPR Article 9 defines special categories of data as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. Notably, special categories of personal data do not include banking information or credit card numbers. Other countries, such as the United States, often consider this type of financial information to be in a special category of sensitive information. Under the GDPR, financial information such as a bank account number is classified as personal data but is not considered a special category of personal data.
Body of Knowledge Domain II, Subdomain A

49. The correct answer is A. The question tells you the data subjects have exercised their right to object. The right to object is available to data subjects when the processing is based on legitimate interests or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In this case, the controller is likely relying on their legitimate interest as the basis for the video surveillance. When data subjects exercise their right to object, the controller must stop the processing unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. GDPR Article 21(1).
Body of Knowledge Domain III, Subdomain B

50. The correct answer is C. Direct marketing is not a compelling justification to continue profiling when the data subject has objected to that processing. Demonstrating legitimate interest requires a balancing test between the purposes of profiling and the rights and freedoms of the data subject. To justify profiling, the balance test would consider the importance of profiling to the controller's particular objective, as well as weigh the interests of the controller against the basis for objection by considering the impact of profiling on the data subject.
Body of Knowledge Domain II, Subdomain F

51. The correct answer is B. Whether the personal data is obtained from the data subject or from another legitimate source, an organisation will need to meet its transparency obligations by providing data subjects with specific information under GDPR Articles 13 and 14 unless an exemption applies. Exemptions apply when:
    - personal data is collected directly from the data subject and the data subject has already been provided with the required information;
    - personal data is obtained from other sources and the data subject has already been provided with the required information;
    - personal data is obtained from other sources and providing the required information to the data subject would be impossible;
    - personal data is obtained from other sources and providing the required information to the data subject would involve a disproportionate effort;
    - personal data is obtained from other sources and providing the required information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
    - you are required by law to obtain or disclose the personal data; or
    - you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

    Body of Knowledge Domain II, Subdomain C

52. The correct answer is A. Museum visitors who signed the consent form are entitled to request that the museum stop using their names and voices via social media, because that use was not included in the consent form. However, the museum should immediately stop using and processing any information for unauthorised uses and not wait for visitors to contact them. Although visitors have a right to request a copy of the images and videos created from their introductions, the consent form specified that these would be deleted after 24 hours and, if handled correctly, should not still be available for a visitor's personal use. Visitors could request monetary compensation for the use of their personal data; however, this does not directly address the reuse of voice data without permission from the data subject. Likewise, although the visitors could ask that the museum stop processing their personal data immediately 'upon receipt' of their request, this does not allow for validation of the request and should not be necessary if the museum was handling the data as specified in the consent form.
Body of Knowledge Domain II, Subdomain F

53. The correct answer is B. In this scenario, Museum4yourSenses is the data controller and therefore they are responsible for establishing the terms of processing in the vendor agreement with the audio-visual company. The audio-visual company is considered the data processor as they are processing personal data on behalf of Museum4yourSenses. Museum4yourSenses is the key decision-maker as they have the overall say and control over the reason and purposes behind data collection and the means and method of any data processing. The vendor is a third party in this scenario and would not have direct communication with the visitors.
Body of Knowledge Domain II, Subdomain A

54. The correct answer is C. Supervisory authorities can enforce data subject rights. The other answer choices lack enforcement ability. When a child is below 16 years old (may be lower as allowed in some member states), the processing of such data may be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
Body of Knowledge Domain II, Subdomain D

55. The correct answer is C. BCRs are legally binding rules and policies that allow a company established in the EU to transfer personal data outside the EU within a multinational company group (such as from a parent company to a subsidiary). Details about BCRs can be found in Article 47 of the GDPR.
Body of Knowledge Domain II, Subdomain I

56. The correct answer is C. While many organisations are adopting the 'as-a-Service' model for delivery of almost everything, as reflected by EaaS (sometimes noted as XaaS), the three common service models for cloud computing are IaaS, PaaS and SaaS.

    IaaS provides computing resources (e.g., storage, servers, hardware and support) remotely. PaaS offers a cloud-based environment in which customers can build, host and deliver their own SaaS applications. SaaS offers software and applications that can be accessed over the internet and are managed by the cloud service provider (CSP) or vendor, not the customer.
    Body of Knowledge Domain III, Subdomain D

57. The correct answer is C. All necessary steps have been taken to mitigate this low-impact breach. The risk assessment is carried out as per GDPR Recitals 76 and 85. The company has taken all steps under Article 33 to ensure that the incident is unlikely to result in a high risk to the affected individuals.
Body of Knowledge Domain II, Subdomain J

58. The correct answer is A. Traditionally, accountability has been part of the Fair Information Practice Principles stating that due diligence and reasonable steps should be undertaken to ensure that personal information will be protected and handled consistently with relevant law and other fair use principles. According to the European Data Protection Supervisor, the GDPR integrates accountability as a principle which requires organisations to put in place appropriate technical and organisational measures and be able to demonstrate and provide evidence of how they complied with the law and the effectiveness of compliance measures.

    Internal allocation of privacy responsibilities and the development of internal policies outlining how data should be processed and handled across the organisational are tools for compliance demonstration. The obligation for controllers to provide data subjects with information about the processing of their personal data allows the organisation to demonstrate transparency, but not necessarily accountability.
    Body of Knowledge Domain II, Subdomain H

59. The correct answer is A. Article 5(1)(e) of the Regulation states that personal data must be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'. An organisation should set the retention period based on how long it will need to retain the data to fulfil the purpose for which it was collected. Other considerations when setting retention periods would include any legal obligations to retain data for a defined period and relevant industry standards and guidelines.
    Body of Knowledge Domain II, Subdomain C

60. The correct answer is B. When personal data is being shared between commercial organisations acting as joint data controllers, it is recommended that they determine their respective responsibilities for compliance with their obligations under the GDPR by means of an arrangement. The determination of their respective responsibilities must address the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controllers' obligations, such as the general data protection principles, legal bases, security measures, data breach notification obligations, data protection impact assessments, the use of processors, third-country transfers and contacts with data subjects and supervisory authorities. The legal form of the arrangement amongst joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a sharing agreement. See GDPR Article 26 and EDPB 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'.
    Body of Knowledge Domain II, Subdomain G

61. The correct answer is C. The 1992 Maastricht Treaty, also known as the Treaty on European Union, is the foundation treaty that created the EU. The Treaty gave EU citizenship to all citizens of the member states. It provided for a central banking system with a common currency and called for greater

cooperation between member states with regard to foreign and security policies, environmental issues, policing and social policies.
Body of Knowledge Domain I, Subdomain C

62. The correct answer is C. Because background check provisions vary across the EU countries, the company would have to analyse its feasibility and possible restrictions on a case-by-case basis. It is important to note that the GDPR does not set specific guidelines for background checks; however, the privacy principles set forth therein must be taken into consideration together with the applicable member state's laws. Additionally, Article 10 of the GDPR states that criminal conviction data may only be processed when authorised under the laws of the applicable member state, or when under the control of an official authority.
Body of Knowledge Domain III, Subdomain A

63. The correct answer is D. In a layered notice, the key information is provided in a short initial notice. More detailed information is available in a subsequent layer should a data subject wish to know more. The EDPB states that the first layer should include the purpose of processing, the controller's identity, and the rights granted by the Regulation, together with information about processing that could surprise or have an impact on the data subject. This layer should enable the data subject to understand what fair processing information is available to them and where it is.
Body of Knowledge Domain II, Subdomain E

64. The correct answer is B. Under Article 15, Isabelle has the right to rectify or erase personal data or restrict processing of personal data concerning herself as well as to object to such processing. Isabelle has the right to lodge a complaint with her local supervisory authority.
Body of Knowledge Domain II, Subdomain F

65. The correct answer is D. As the data controller, Novatours, after confirming Isabelle's identity, must stop processing her data without undue delay and if requested, erase Isabelle's personal data. Article 17 of the GDPR requires controllers to limit or erase personal information without undue delay when provisions for multiple grounds exist, including if Isabelle withdrew her consent, the personal data was unlawfully processed, or personal data was collected in relation to the offer of information services for a child at least 16 years old. The verification processes do not require multi-factor authentication, have no time constraint, and do not require that requests come from a supervisory authority in order to be honoured.
Body of Knowledge Domain II, Subdomain F

66. The correct answer is A. Article 12(3) of the GDPR details how an organisation must handle a data subject request and what is expected from the controller. This includes the requirement that a controller receiving such a request must respond within 30 days. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The controller shall inform the data subject of any such extension within one month of receipt of the request together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless

otherwise requested by the data subject. Not all requests may be honoured; some requests may be considered excessive and therefore may not be accepted.
Body of Knowledge Domain II, Subdomain F

67. The correct answer is D. While Article 32 of the GDPR sets forth the circumstances that constitute a breach, Article 33 includes the notification requirements for when a breach occurs. According to the WP29 guidance, 'As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records'. Since the loss of accessibility to customer data was limited to a few hours, and did not result in harm to data subjects, it is sufficient for Company Z to document the specifics of the situation.
Body of Knowledge Domain II, Subdomain H

68. The correct answer is C. Convention 108, also known as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, is a Council of Europe Treaty. Despite its name, the Council of Europe is an international human rights organisation and is not limited to participation by European Union countries or countries located within the continent of Europe. Directive 95/46/EC, the Treaty of Lisbon, and the Charter of Fundamental Rights of the European Union only apply to countries within the EU.
Body of Knowledge Domain I, Subdomain C

69. The correct answer is A. Data protection by design (privacy by design) should be applied to the entire life cycle of a project. In this manner, organisations can provide the best policies, procedures and technologies to respect individuals' privacy, protect personal data appropriately, and still provide accessibility to the personal data as necessary and appropriate.
Body of Knowledge Domain II, Subdomain H

70. The correct answer is A. A request may be manifestly unfounded if, as in this example, the individual clearly has no intention to exercise their right of access – here, they are willing to take compensation to withdraw the request. A request also can be manifestly unfounded if it is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. Analysing requests for being manifestly unfounded is not a mechanical process. The request must be considered in the context in which it is made. If the individual genuinely wants to exercise their rights, it is unlikely that the request is manifestly unfounded.
Body of Knowledge Domain II, Subdomain F

71. The correct answer is C. Individuals are free to choose the option to pursue in exercising their rights under the GDPR in cases of noncompliance. They can pursue litigation in accordance with their national laws, complain to their regulator, or, indeed, they can pursue both remedies at the same time. They can do so regardless of whether they have complained to the controller or processor. Please refer to GDPR Articles 77–79.
Body of Knowledge Domain II, Subdomain K

72. The correct answer is A. Automated decision-making that would otherwise be prohibited is allowed if it is authorised by law, is based on the data subject's explicit consent, or is necessary for the preparation and execution of a contract. Because automated decision-making increases the risk for harmful profiling, the GDPR generally prohibits fully automated decision-making in most other cases. The risk may be mitigated by human involvement provided such involvement has a direct influence on the result of the processing. Data subjects cannot object to automated decision-making unless it produces legal effects concerning the data subject or similarly affects them in a significant way. Because of the risks associated with automated decision-making, data subjects do not have to formally object to such processing as a condition of benefiting from it.
Body of Knowledge Domain II, Subdomain F

73. The correct answer is A. The recipient's prior consent is required and must be given to the sender. There is a limited exception for an existing customer relationship when offering similar products or services. Individuals must be given an opportunity to opt out of direct marketing at the time their personal data is collected. If they do not opt out, recipients must be given on each communication an opportunity to opt out (unsubscribe). The lawful basis will be legitimate interest.
Body of Knowledge Domain II, Subdomain C

74. The correct answer is A. Data subjects are not entitled to know about the risk of security breaches; they are only entitled to be informed when there is an actual breach involving their personal data. Data processors are subject to joint and several liability. If one of the controllers or processors involved pays the data subject the full amount of damages, the controller or processor can then seek contribution from other parties. While it is likely that data subjects will start any complaint process by contacting the applicable controller, doing so is not a mandatory first step.
Body of Knowledge Domain II, Subdomain K

75. The correct answer is B. GDPR Article 83 states that without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each member state may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that member state. If a violation affects individuals in more than one member state, a company could be fined by each member state according to its rules. This could result in a very significant financial impact on any company found violating fair notice requirements.
Body of Knowledge Domain II, Subdomain J

76. The correct answer is A. Article 33 of the GDPR sets out the requirements for notification of personal data breaches: 'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, provide notification to the supervisory authority competent, as described in Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons'.
Body of Knowledge Domain II, Subdomain G

77. The correct answer is D. While the Regulation does not state how to comply, it does state that 'the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are

processed'. Data minimisation is one of the key Fair Information Practices (FIPs) emphasised by privacy by design/default.
Body of Knowledge Domain II, Subdomain H

78. The correct answer is C. There are a number of key matters that should be addressed in an internal privacy policy including scope, policy statement, employee responsibility, management responsibility, reporting incidents and policy compliance. These matters will weave in the GDPR principles for processing personal data. The policy itself should reflect how those principles are applied by restaurant employees and app administrators.
Body of Knowledge Domain II, Subdomain H

79. The correct answer is D. Convention 108 is a legally binding treaty for the member states of the Council of Europe and any other country that signs on to the treaty. The OECD Guidelines, APEC Privacy Framework, and UN Declaration are not legally binding instruments but instead offer guidance to organisations and governments.
Body of Knowledge Domain I, Subdomain C

80. The correct answer is C. Any data collected by a non-EU controller from persons in the EU is subject to GDPR, even if it is pseudonymised. However, any data collected by a non-EU controller from persons outside of the EU is not subject to the GDPR. However, it may be subject to applicable laws in the relevant country of origin.
Body of Knowledge Domain II, Subdomain B

81. The correct answer is B. The Lisbon Treaty of 2007 significantly affected the data protection framework and amended many of the provisions of the Treaty on European Union and the Treaty Establishing the European Community. It recognised the protection of personal data as a fundamental right and made the Charter of Fundamental Rights a legally enforceable document.
Body of Knowledge Domain I, Subdomain B

82. The correct answer is A. Article 45 of the GDPR states the requirements the European Commission must take into consideration regarding adequacy decisions. Articles 46 and 47 set forth alternate means of transferring data, including legally binding instruments with authorities, standard contractual clauses and binding corporate rules. However, there are situations where neither Article applies and yet data transfers must occur, e.g., intra-group transfers within an international organisational group. For these limited and specific situations, Article 49 sets forth derogations which may be utilised provided certain conditions are met.
Body of Knowledge Domain II, Subdomain I

83. The correct answer is C. The GDPR makes it mandatory for companies to undertake a DPIA for any new projects that are likely to create 'high risks' or before proceeding with 'risky' personal data processing. Implementing surveillance cameras outside will systematically monitor a publicly accessible area on a large scale. Further we are unsure how they will identify possible bank thieves. Could this identification incorrectly profile people as thieves? There are several situations in the bank

scenario that would require a DPIA to understand risks. The other scenarios in this question do not pose high risks to individuals and thus would not require a DPIA.
Body of Knowledge Domain II, Subdomain H

84. The correct answer is D. If the original purpose for processing and retaining the personal data has expired, it should be securely deleted or anonymised so that it is no longer 'in a form which permits identification of data subjects'. The personal data was collected to administer the webinar, not to maintain a CRM database. Personal data can only be retained indefinitely if it is being held for:
    - archiving purposes in the public interest;
    - scientific or historical research purposes; or
    - statistical purposes.

    Body of Knowledge Domain II, Subdomain C

85. The correct answer is C. The cameras are fake and therefore are not collecting any personal data, therefore the GDPR does not apply. This example is mentioned in the European Data Protection Board's (EDPB) 'Guidelines 3/2019 on processing of personal data through video devices' which states that although the GDPR does not apply, in some member states the situation might be subject to other legislation.
    Body of Knowledge Domain III, Subdomain B

86. The correct answer is A. The GDPR applies to any personal data that is structured – in other words, it applies to personal data that is included in a filing system, whether digital or in hard copy. If the data is not organised in any way (for example, an untagged pile of documents), there is no system and, therefore, the GDPR would not apply. This is a key reason why it is essential to have internal hard copies organised or catalogued in a way that is accessible according to specific criteria, so that adequate protections can be offered to data subjects.
    Body of Knowledge Domain II, Subdomain B

87. The correct answer is C. The European Commission has the power to determine whether a country outside the EU offers an adequate level of data protection. 'Adequate' third countries are those for which the Commission has confirmed an 'essentially equivalent' level of data protection. In those countries, national laws provide a level of protection for personal data that is comparable to EU law.
    Body of Knowledge Domain II, Subdomain I

88. The correct answer is D. Under the Data Protection Directive, transparency was expressly linked to the concept of fairness of processing. The GDPR retains this link, explaining that 'the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes'. Failure to provide fair processing information where required by the Regulation, or failure to process personal data in accordance with the information provided, is therefore likely to render the processing unfair, as well as to constitute a violation of a number of the Regulation's specific information provision obligations.
    Body of Knowledge Domain II, Subdomain E

89. The correct answer is B. GDPR Article 8 – 'Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states may provide by law for a lower age for those purposes provided that such lower age is not below 13 years'.
Body of Knowledge Domain II, Subdomain D

90. The correct answer is A. The concept of fairness is linked to the idea that the data subject must be informed of the existence of the processing operation and its purpose. A privacy notice is used to provide individuals with information about who is processing their personal data and how and why their data will be used.
Body of Knowledge Domain II, Subdomain C

iapp

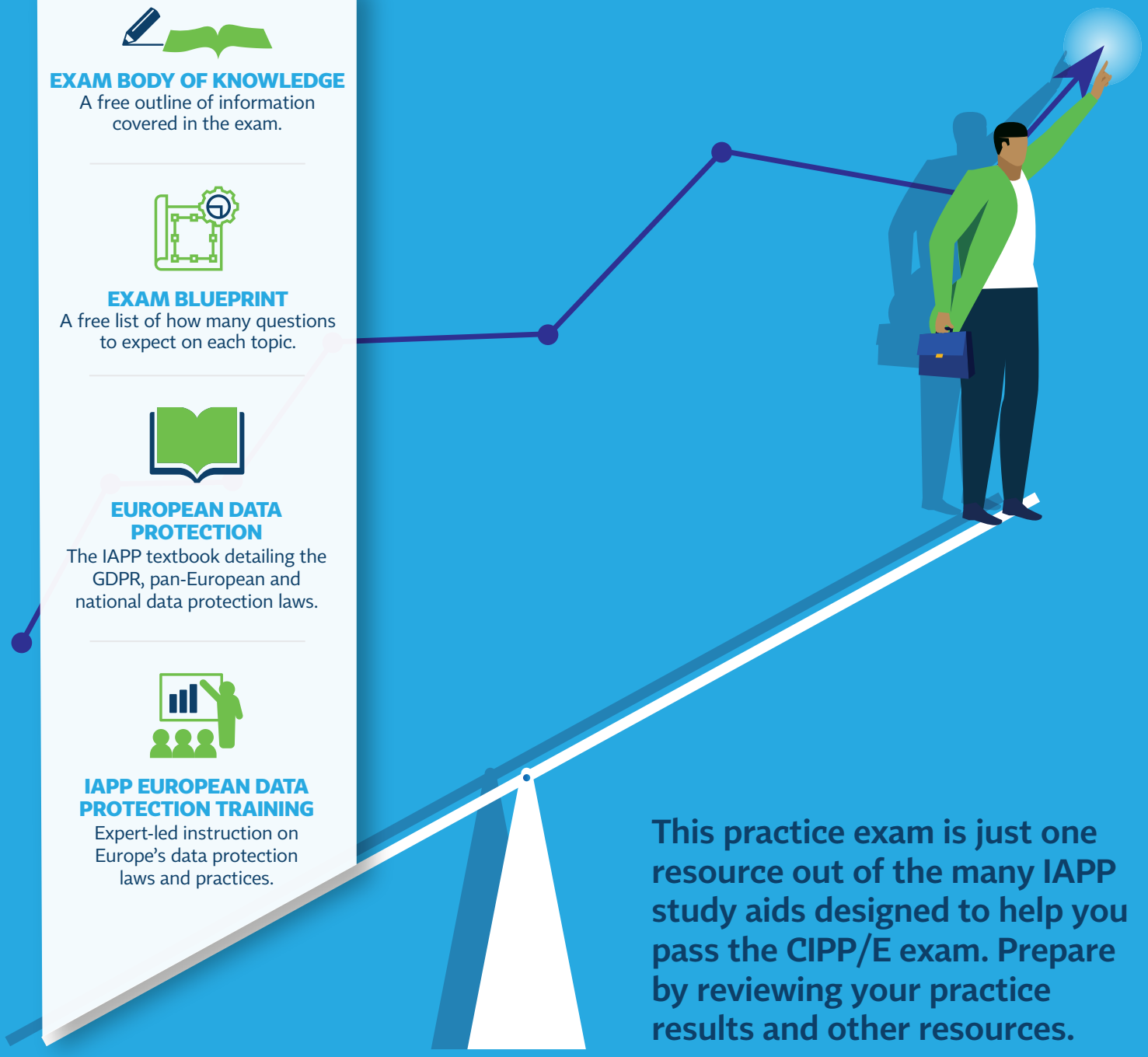
Build on Your Practice Exam Results

EXAM BODY OF KNOWLEDGE
A free outline of information covered in the exam.

EXAM BLUEPRINT
A free list of how many questions to expect on each topic.

EUROPEAN DATA PROTECTION
The IAPP textbook detailing the GDPR, pan-European and national data protection laws.

IAPP EUROPEAN DATA PROTECTION TRAINING
Expert-led instruction on Europe's data protection laws and practices.



This practice exam is just one resource out of the many IAPP study aids designed to help you pass the CIPP/E exam. Prepare by reviewing your practice results and other resources.

Go to **iapp.org/train** to find these and other resources that will help you feel confident and prepared for your CIPP/E exam.