Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

IAPP-CIPP-E MCQs
IAPP-CIPP-E TestPrep
IAPP-CIPP-E Study Guide
IAPP-CIPP-E Practice Test
IAPP-CIPP-E Exam Questions

killexams.com

IAPP

IAPP-CIPP-E

Certified Information Privacy Professional/Europe (CIPP/E)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/IAPP-CIPP-E

Question: 727

SCENARIO:
TechTrend Inc., a cloud service provider based in the EU, transfers customer data to a subcontractor in a third country without an adequacy decision. The transfer is based on Standard Contractual Clauses (SCCs) post-Schrems II. During an audit, the supervisory authority questions whether TechTrend conducted a Transfer Impact Assessment (TIA) as recommended by the EDPB. What is the most critical factor TechTrend must evaluate in the TIA to ensure GDPR compliance?

A. The financial stability of the subcontractor to ensure long-term compliance
B. The volume of data transferred to the third country
C. The subcontractor's ISO 27001 certification status
D. The likelihood of government access to data in the third country

Answer: D

Explanation: Following the Schrems II ruling and EDPB Recommendations 01/2020 on Supplementary Measures, a Transfer Impact Assessment is essential when using SCCs for data transfers to third countries. The TIA must primarily assess the risk of government access to personal data in the recipient country, including laws and practices that may undermine GDPR protections. This is critical to determining whether additional safeguards are needed to ensure compliance.

Question: 728

CloudSafe, a cloud provider, suffers a breach on May 1, 2026, at 10:00 UTC, exposing customer names and addresses. The risk assessment estimates a 0.3 probability of phishing risks (impact: 6/10). Under Articles 33 and 34, what must CloudSafe do?

A. Notify the supervisory authority within 72 hours
B. Notify customers and the supervisory authority immediately
C. Document the breach without notifications
D. Notify customers only if phishing occurs

Answer: A

Explanation: Article 33 requires notifying the supervisory authority within 72 hours unless the breach is unlikely to result in a risk. Article 34 requires notifying data subjects only for high risks. The moderate risk (0.3 probability, 6/10 impact) warrants authority notification but not customer notification. Documentation is required, but notification to the authority is mandatory.

Question: 729

SCENARIO
SmartCity, a municipal authority in Portugal, deploys a surveillance system using facial recognition to monitor public spaces for security. The system processes biometric data of residents without their explicit consent, relying on public interest as the legal basis. SmartCity conducts a DPIA, which identifies high risks but concludes that security benefits outweigh them. A resident challenges the system, arguing that it violates GDPR due to inadequate safeguards. SmartCity's DPO, Ana, must assess the compliance issues.

What is the most significant GDPR compliance issue with SmartCity's facial recognition system?

A. Lack of consultation with the supervisory authority prior to deployment
B. Insufficient safeguards to mitigate risks identified in the DPIA
C. Failure to notify residents about the use of facial recognition technology
D. Relying on public interest instead of explicit consent for biometric data processing

Answer: D

Explanation: Biometric data processing for identification in public spaces is a special category of data under GDPR Article 9(1), requiring explicit consent or another strict condition (e.g., substantial public interest under Article 9(2)(g) with a basis in Union or Member State law). Public interest alone, without specific legal authorization, is insufficient, making this the most significant violation. While inadequate safeguards, lack of notification, and failure to consult (Article 36) are also issues, the absence of a proper legal basis for processing biometric data is the core compliance gap.

Question: 730

A privacy scholar is analyzing the influence of national data protection laws in Europe before the GDPR's adoption in 2016. The scholar focuses on Germany's Bundesdatenschutzgesetz (BDSG) of 1977, which was a pioneering law. The scholar's research reveals that the German Federal Constitutional Court's 1983 Census Decision reinforced a key concept derived from the BDSG. Which concept, later influential in GDPR's development, emerged from this decision?

A. Data sovereignty
B. Purpose limitation
C. Informational self-determination
D. Transparency obligations

Answer: C

Explanation: The 1983 Census Decision by Germany's Federal Constitutional Court established the right to informational self-determination, emphasizing individuals' control over their personal data. This concept, rooted in the BDSG, influenced European data protection frameworks, including the GDPR. Data sovereignty is not a legal term here, and purpose limitation and transparency, while important, were

not the primary focus of the decision.

Question: 731

The EDPB issues a binding decision in 2024, fining AutoDrive, a Czech company, €6 million for transferring driver data to China without safeguards, violating Article 44. The decision follows a dispute between the Czech LSA and German CSA. Binding only on the Czech DPA
B. Advisory, subject to CJEU review
C. Per Article 65, what is the legal status of this decision?
C. Binding on all DPAs and AutoDrive
D. Subject to national court appeal

Answer: C

Explanation: Article 65 empowers the EDPB to issue binding decisions in LSA-CSA disputes, enforceable on all DPAs and the controller (AutoDrive). The decision is not advisory, limited to one DPA, or automatically subject to national court appeal, though AutoDrive may seek judicial review under EU law.

Question: 732

A Bulgarian e-commerce platform uses profiling to offer personalized discounts, relying on consent. A customer withdraws consent but wants to continue receiving discounts. Under GDPR Article 7, what must the platform do?

A. Conduct a DPIA to justify continued profiling.
B. Continue profiling based on legitimate interests.
C. Notify the supervisory authority of the consent withdrawal.
D. Cease profiling and assess alternative legal bases for continued discounts.

Answer: D

Explanation: GDPR Article 7 allows data subjects to withdraw consent at any time, requiring the controller to cease processing based on consent. The platform must stop profiling and evaluate whether another legal basis (e.g., contract necessity) allows continued discounts. Legitimate interests are unlikely to apply for marketing profiling, and notification or a DPIA is not directly required.
Reference: GDPR Article 7

Question: 733

A tech startup in Denmark develops a fitness app that collects user data, including heart rate and exercise logs, to provide personalized workout plans. The startup shares this data with a U.S.-based processor under a data processing agreement with standard contractual clauses (SCCs). During a GDPR audit, the

supervisory authority questions the transfer's compliance. What must the startup do to ensure GDPR-compliant transfers?

A. Ensure the processor is ISO 27001 certified
B. Obtain explicit user consent for the transfer
C. Conduct a transfer impact assessment (TIA) to evaluate U.S. data protection laws
D. Rely on the processor's privacy policy for compliance

Answer: C

Explanation: Following the Schrems II ruling, GDPR Article 46 requires a TIA to assess the recipient country's legal framework (e.g., U.S. surveillance laws) and implement supplementary measures (e.g., encryption) alongside SCCs to ensure equivalent protection. Consent is impractical for app users, and ISO 27001 or privacy policies do not meet GDPR transfer requirements.

Question: 734

A French company uses a processor in Singapore for payroll services. The processor signs Standard Contractual Clauses (SCCs) but fails to encrypt data in transit, leading to a breach affecting 10,000 employees. According to EDPB Guidelines 01/2021, what is the controller's primary obligation under GDPR?

A. Conduct a DPIA to assess cross-border risks
B. Notify the CNIL within 72 hours of the breach
C. Terminate the processor contract immediately
D. Implement supplementary measures for SCCs

Answer: B

Explanation: GDPR Article 33 requires the controller to notify the supervisory authority (CNIL in France) within 72 hours of a personal data breach unless it is unlikely to result in a risk. The EDPB Guidelines emphasize timely notification for breaches involving sensitive data like payroll.

Question: 735

A retail company in Portugal collects customer data, including names and purchase histories, for a loyalty program. The company shares this data with a marketing processor under a data processing agreement. During a cyberattack, the processor's database is compromised, exposing customer data. Under GDPR, what is the processor's primary obligation upon discovering the breach?

A. Conduct an internal investigation before notification
B. Notify the supervisory authority within 72 hours
C. Encrypt the compromised data to mitigate risks
D. Notify the controller without undue delay

Answer: D

Explanation: GDPR Article 33(2) mandates that a data processor notify the data controller without undue delay after becoming aware of a personal data breach. The processor's role is to inform the retail company, which, as the controller, must assess the breach and notify the supervisory authority (Article 33(1)) and data subjects (Article 34) if required. Encryption or investigation may follow but is not the primary obligation.

Question: 736

SCENARIO
EduTech, a Finnish ed-tech company, partners with CloudLearn, a Canadian firm, to store student data. EduTech relies on an adequacy decision for Canada but fails to monitor ongoing compliance. After a data breach at CloudLearn, the Finnish supervisory authority finds that Canada's data protection laws have weakened. A student files a complaint.

What is the key GDPR issue in this scenario?

A. Lack of a data processing agreement with CloudLearn
B. Failure to monitor the validity of Canada's adequacy decision
C. Inadequate security measures at CloudLearn
D. Absence of a Data Protection Impact Assessment (DPIA)

Answer: B

Explanation: GDPR Article 45 requires controllers to ensure that adequacy decisions remain valid, as changes in third-country laws may necessitate additional safeguards. EduTech's failure to monitor Canada's compliance is the primary violation. A data processing agreement, security measures, and DPIA are relevant but secondary to the adequacy issue.

Question: 737

A Greek hospital processes patient data for treatment, relying on Article 6(1)(c) (legal obligation) and Article 9(2)(h) (healthcare). It also shares anonymized data with a research institute without informing patients, claiming no GDPR obligation applies. A supervisory authority audit reveals that the anonymization process retains indirect identifiers, risking re-identification. Which GDPR principle is at risk?

A. Accountability
B. Lawfulness, fairness, and transparency
C. Data minimization
D. Storage limitation

Answer: B

Explanation: Article 5(1)(a) requires lawful, fair, and transparent processing. Sharing data that is not fully anonymized (due to re-identification risks) constitutes personal data processing under GDPR, requiring a legal basis and transparency. The hospital's failure to inform patients and ensure proper anonymization breaches transparency and lawfulness.

Question: 738

A multinational e-commerce company, headquartered in the EU, operates a loyalty program requiring customers to consent to the processing of their purchase history and browsing behavior for personalized marketing. The consent form is embedded in a lengthy terms-of-service agreement, pre-checked, and requires users to agree to all terms to proceed with account creation. The company claims this satisfies GDPR's requirement for freely given, specific, informed, and unambiguous consent. During a compliance audit, a Data Protection Authority (DPA) reviews the consent mechanism. Which of the following best describes the GDPR compliance status of this consent process?

A. Non-compliant, as the consent form is not displayed prominently
B. Compliant, as users can proceed only after agreeing to the terms
C. Compliant, as the consent is embedded in a legally binding agreement
D. Non-compliant, as consent is bundled with other terms and not granular

Answer: D

Explanation: Under GDPR Article 4(11), consent must be freely given, specific, informed, and unambiguous. Bundling consent with other terms, such as in a terms-of-service agreement, violates the requirement for specific consent, as users cannot choose data processing independently. Pre-checked boxes fail to meet the unambiguous requirement, as affirmative action is needed. The consent must also be granular, allowing users to consent to specific purposes separately.

Question: 739

SCENARIO
MediCare, a Belgian hospital, uses an AI system developed by HealthTech, a Swedish company, to predict patient outcomes based on medical records. The AI processes sensitive health data and requires continuous data sharing between MediCare and HealthTech. Both act as joint controllers, but their agreement lacks details on data subject rights handling. A patient requests access to their data processed by the AI, but MediCare denies the request, claiming HealthTech is responsible. The patient escalates the issue to the Belgian supervisory authority.

What is the key GDPR non-compliance issue in this scenario?

A. Absence of a Data Protection Impact Assessment (DPIA) for AI processing
B. Inadequate security measures for data shared with HealthTech

C. Lack of a lawful basis for processing health data in the AI system
D. Failure to define responsibilities for handling data subject rights in the joint controller agreement

Answer: D

Explanation: Under Article 26 GDPR, joint controllers must define their respective responsibilities for complying with GDPR obligations, including handling data subject rights, in a transparent agreement. MediCare's denial of the access request and shifting responsibility to HealthTech indicates a failure to comply with this requirement. While a DPIA is likely required for AI processing, the scenario focuses on the access request issue. The lawful basis and security measures are not directly implicated.

Question: 740

SCENARIO
BankPro, a Maltese bank, uses a third-party vendor, PayCorp, in Russia, to process payments. BankPro implements SCCs but fails to assess Russia's surveillance laws. A breach at PayCorp exposes data, leading to a complaint with the Maltese supervisory authority.

What is the primary GDPR violation?

A. Lack of a Data Protection Impact Assessment (DPIA)
B. Failure to conduct a Transfer Impact Assessment (TIA) for Russia
C. Inadequate encryption of payment data
D. Absence of a data processing agreement

Answer: B

Explanation: Schrems II requires a TIA to assess third-country surveillance laws (Article 46). BankPro's failure to evaluate Russia's laws is the primary violation. DPIA, encryption, and a data processing agreement are not the focus.

Question: 741

A UK-based cloud provider processes personal data for an EU client under a contract that specifies compliance with GDPR Article 5 principles. The client discovers that the provider has retained outdated customer data beyond the agreed retention period, violating the storage limitation principle. What is the consequence for the cloud provider under GDPR?

A. No liability, as the client is the data controller
B. Joint liability with the client for the violation
C. Sole liability for breaching Article 5
D. Exemption, as retention is a technical issue

Answer: B

Explanation: Under GDPR Article 28, a data processor (cloud provider) must process data only as instructed by the data controller (client). However, both controller and processor share responsibility for ensuring compliance with Article 5 principles, including storage limitation. A breach of this principle can result in joint liability, with fines up to €20 million or 4% of annual global turnover, as per Article 83.

Question: 742

PharmaGlobal, a Belgian company, transfers clinical trial data to a research partner in Japan. The European Commission has granted Japan an adequacy decision under GDPR Article 45. During a compliance audit, the Belgian DPA questions whether PharmaGlobal conducted a Transfer Impact Assessment (TIA) despite the adequacy decision. Per EDPB Recommendations 01/2020, what is PharmaGlobal's obligation regarding a TIA?

A. Perform a TIA to confirm Japan's laws align with the adequacy decision
B. Conduct a TIA only if the data includes special categories like health data
C. No TIA is required, as Japan's adequacy decision ensures sufficient protection
D. Suspend transfers until a TIA is completed and approved by the DPA

Answer: C

Explanation: GDPR Article 45 allows data transfers to countries with an adequacy decision without further safeguards. EDPB Recommendations 01/2020 clarify that a TIA is unnecessary for transfers to adequate jurisdictions like Japan, as the European Commission's decision confirms sufficient protection. A TIA for special categories or to confirm laws is not required. Suspending transfers is unwarranted given the adequacy decision.

Question: 743

A Swedish marketing firm collects user data through a mobile app to target advertisements. The app tracks location data, which reveals users' religious habits, without specifying this in its privacy notice. Under GDPR Article 13, what is the firm's obligation?

A. Cease processing location data until a data protection impact assessment is conducted.
B. Update the privacy notice to include the processing of religious data and obtain consent.
C. Notify the supervisory authority of the processing of special category data.
D. Rely on legitimate interests for processing without updating the privacy notice.

Answer: B

Explanation: GDPR Article 13 requires controllers to provide transparent information about the processing of personal data, including the categories of data and purposes, at the time of collection. Location data revealing religious habits qualifies as special category data under Article 9, requiring explicit consent. The firm must update its privacy notice to reflect this processing and obtain consent.

Legitimate interests cannot justify processing special category data without consent.
Reference: GDPR Articles 13, 9;

Question: 744

A Luxembourg-based company in 2026 is investigated for processing employee health data without a lawful basis, allegedly violating GDPR and Article 8 of the EU Charter. The company cites Niemietz v. Germany (1992) to argue that workplace data is exempt from privacy protections. Which aspect of Niemietz would undermine the company's argument?

A. Health data is not covered by Article 8
B. Private life extends to professional activities
C. Employers have unrestricted data processing rights
D. Workplace data is exempt from ECHR protections

Answer: B

Explanation: In Niemietz v. Germany (1992), the ECtHR ruled that Article 8's right to private life extends to professional activities, including the workplace, undermining the company's exemption claim. Health data is protected, employers' rights are limited, and workplace data is not exempt.

Question: 745

A multinational corporation based in the EU, DataFlow Inc., regularly transfers personal data to its U.S. subsidiary for processing customer analytics. Following the Schrems II ruling, the company relies on Standard Contractual Clauses (SCCs) to legitimize these transfers. During a compliance audit, the European Data Protection Board (EDPB) requests a Transfer Impact Assessment (TIA) to evaluate the effectiveness of SCCs. The TIA reveals that U.S. surveillance laws, including Section 702 of the FISA Amendments Act, may allow access to EU citizens' data without adequate redress mechanisms. According to GDPR Article 46 and EDPB Recommendations 01/2020, what must DataFlow Inc. do to ensure compliance with GDPR Chapter V for these data transfers?

A. Continue transfers without changes, as SCCs are inherently sufficient under GDPR
B. Suspend data transfers to the U.S. unless supplementary measures ensure an essentially equivalent level of protection
C. Obtain explicit consent from data subjects for each transfer under Article 49
D. Rely on the EU-U.S. Data Privacy Framework (DPF) without further assessment

Answer: B

Explanation: The Schrems II ruling invalidated the EU-U.S. Privacy Shield and emphasized that SCCs require a case-by-case assessment to ensure an essentially equivalent level of protection as guaranteed by GDPR. EDPB Recommendations 01/2020 mandate a TIA to evaluate third-country laws, such as U.S. surveillance laws, that may undermine SCC protections. If the TIA indicates inadequate protections,

supplementary measures (technical, contractual, or organizational) must be implemented. If these measures cannot ensure equivalence, transfers must be suspended. Consent under Article 49 is not suitable for regular transfers, and the DPF requires its own assessment, not automatic reliance.

Question: 746

A gaming company in the UK processes players' personal data, including usernames, email addresses, and in-game purchases, to enhance user experience. The company uses a cloud-based processor in the EU to analyze gameplay data. The processor's contract includes standard contractual clauses (SCCs) but lacks provisions for sub-processor engagement. Under GDPR Article 28, what is the company's primary obligation as the data controller?

A. Verify the processor's ISO 27001 certification
B. Conduct a transfer impact assessment (TIA) for EU-based processing
C. Require the processor to appoint a Data Protection Officer (DPO)
D. Ensure the processor obtains controller approval for sub-processors

Answer: D

Explanation: GDPR Article 28(2) requires that a processor only engage sub-processors with the controller's prior authorization, as specified in the data processing agreement. The gaming company must ensure the contract includes provisions for approving sub-processors to maintain control over data processing. A TIA is relevant for non-EU transfers, not EU-based processing, and DPO or ISO 27001 requirements are not mandated by Article 28.

Question: 747

A Belgian insurer uses automated decision-making (ADM) to deny claims based on algorithmic risk scores, citing legitimate interests. A claimant challenges the decision under GDPR Article 22. What is the insurer's strongest defense to continue ADM?

A. Legitimate interests override data subject rights
B. The claimant provided explicit consent
C. Human oversight mitigates Article 22 restrictions
D. The decision is necessary for contract performance

Answer: D

Explanation: GDPR Article 22 prohibits ADM producing legal effects unless it is necessary for entering or performing a contract (Article 22(2)(a)), authorized by law, or based on explicit consent. Insurance claim decisions may qualify as contractual necessity if essential to the contract.

Question: 748

NewsCorp, a media company, processes subscriber data for personalized content recommendations. A subscriber, Chloe, objects to processing for recommendations under Article 21, citing irrelevant suggestions. The legal basis is Article 6(1)(f) (legitimate interests), and the recommendation algorithm uses a relevance score: Score = 0.5 × Click_Rate + 0.3 × Time_Spent + 0.2 × Category_Preference. How must NewsCorp respond?

A. Stop processing Chloe's data for recommendations
B. Adjust the algorithm to improve relevance
C. Continue processing, as legitimate interests apply
D. Retain the data but pause recommendations temporarily

Answer: A

Explanation: Article 21 allows data subjects to object to processing based on legitimate interests, and for direct marketing (including personalized recommendations), the objection is absolute. NewsCorp must cease processing Chloe's data for recommendations, regardless of the algorithm's design or legitimate interests. Adjusting the algorithm or pausing processing does not fully comply with the objection.

Question: 749

SCENARIO
EduOnline, an e-learning platform in Portugal, uses a third-party vendor, StudyCloud, based in India, to host student data (names, grades, and learning analytics). The data is transferred under SCCs, but EduOnline does not assess India's surveillance laws. StudyCloud uses the data for an unauthorized AI research project. A student complains to the Portuguese Data Protection Authority about misuse of their data. EduOnline's DPO, Miguel, must evaluate the GDPR violations.

What is the most significant GDPR violation by StudyCloud?

A. Using student data for an unauthorized AI research project
B. Failure to notify EduOnline of the AI research
C. Lack of supplementary measures for India data transfers
D. Absence of encryption for student data

Answer: A

Explanation: GDPR Article 5(1)(b) requires that personal data be processed for specified purposes and not used in a manner incompatible with those purposes. StudyCloud's use of student data for an unauthorized AI research project violates this purpose limitation principle and lacks a legal basis (Article 6). This is the most significant violation, as it directly addresses the student's complaint about data misuse. Notification, transfer safeguards, and encryption are also issues, but the purpose limitation violation is the most severe.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.