Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

KILL EXAMS

PDPF Practice Questions
PDPF Practice Test
PDPF Practice Exam
PDPF Exam Questions
PDPF Study Guide

PASS

killexams.com

Exin

PDPF

Privacy and Data Protection Foundation

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/PDPF

Question: 1465

An organization has been informed of a potential data breach. What is the timeline for notifying the supervisory authority?

A. There is no specific timeline
B. Within 24 hours
C. Within one week
D. Within 72 hours

Answer: D
Explanation: The organization is required to notify the supervisory authority of a potential data breach within 72 hours of becoming aware of it. This prompt reporting helps regulatory authorities assess the situation and take necessary actions to protect data subjects.

Question: 1466

A 2026 AI ethics board reviews Bulgarian firm's sentiment analysis on employee feedback from Romania and Serbia (non-EU). Romanian adds consent. Definition?

A. Privacy as ethical, standardizing.
B. Privacy as emotional shield, data protection exempting analysis.
C. Privacy as feedback control, relating via consents in Union review.
D. Privacy as national sentiment, Romanian adds.

Answer: C
Explanation: Privacy controls emotional data (Recital 71), with data protection's consent (Article 6(1)(a)) integrating Romanian adds in Union AI boards for ethical processing.

Question: 1467

A healthcare organization is developing a new patient records system. They want to ensure that

patients can easily access their own data. Which aspect of Privacy by Design does this prioritize?

A. User empowerment
B. Transparency and accountability
C. Security by design
D. Data minimization

Answer: A
Explanation: Prioritizing patient access to their own data aligns with user empowerment, a key aspect of Privacy by Design. This approach allows individuals to have control over their personal information and fosters trust in the healthcare organization.

Question: 1468

A data subject has requested to withdraw their consent for data processing. What is the organization's obligation regarding this request?

A. The organization must comply with the request and cease processing the data
B. The organization must inform the data subject that consent cannot be withdrawn
C. The organization can continue processing the data until the end of the month
D. The organization can refuse the request if the data is necessary for a contract

Answer: A
Explanation: The organization is obligated to comply with the data subject's request to withdraw consent and must cease processing the data immediately. This ensures that individuals retain control over their personal information.

Question: 1469

A data protection audit team plans to assess the effectiveness of technical and organizational measures. Which method is most appropriate?

A. Conducting a social media marketing analysis

B. Reviewing the company's annual profit and loss statements
C. Interviewing stakeholders, reviewing policies, and testing controls in practice
D. Organizing a company-wide party to boost morale

Answer: C
Explanation: Assessing measures involves qualitative and quantitative evaluation through interviews, policy review, and practical testing to verify the adequacy and effectiveness of controls in protecting personal data.

Question: 1470

A Cypriot tourism aggregator's booking platform, integrating hotel APIs across EU islands, processes inferred family statuses from reservations, vulnerable to API leaks. What underscores data protection's resilience importance?

A. Sharing raw inferences with partners under broad consents
B. Building API security and mapping into core architecture, fortifying against leaks to maintain operational continuity
C. Implementing after major incidents, using them for insurance claims
D. Auditing annually only, aligning with low-frequency travel cycles

Answer: B
Explanation: Inferences create personal data risks; protection's role is resilience via security (Article 32) and mapping (Article 30), preventing leaks that halt bookings and incur fines. Reactive insurance secondary; broad consents invalid (Article 7); annual audits insufficient for dynamic APIs—embedded fortification ensures uptime and compliance.

Question: 1471

B2C site embeds Twitter Timeline widget with data collection enabled, scraping follows for interest graphs sold to partners. Widget ignores Do Not Track. Primary breach?

A. Follows public non-personal interests
B. DNT voluntary non-binding signal
C. Widgets informational exempt tracking
D. Processing public data absent lawful basis

Answer: D
Explanation: Public data still requires basis for marketing (consent/interest); widgets track cross-site. Internet widgets covertly profile.

Question: 1472

A Maltese gaming app in 2026 monitors playstyles via device sensors, inferring addictions linked to health vulnerabilities from session patterns. Data shared with therapists. What distinction from standard play data applies, and what sharing condition fails?

A. Sensors as non-personal telemetry, free sharing.
B. Sessions as contractual, no conditions.
C. Patterns as standard metrics, sharing under consent.
D. Health inferences as special, needing explicit for therapy sharing.

Answer: D
Explanation: Inferred health data (Article 9(1)(b)) requires explicit consent (Article 9(2)(a)) for sharing, beyond standard data (Article 4(1)). Purpose limitation (Article 5(1)(b)) demands specified recipients. DPIA for addiction profiling is required, per 2024 EDPB gaming opinions.

Question: 1473

A software company is developing a new product that requires users to input personal data. To enhance user trust, they decide to implement strong data encryption measures. This decision reflects which aspect of Privacy by Design?

A. Security by default
B. Data integrity and security

C. User control over personal data
D. Proactive measures

Answer: B
Explanation: Implementing strong data encryption measures is a proactive approach to ensuring data integrity and security. This aspect of Privacy by Design focuses on protecting personal data from unauthorized access and ensuring that it remains confidential.

Question: 1474

Under GDPR privacy regs, a Romanian drone delivery service processes real-time location for 4,000 urban flights. What 2026 development constrains?

A. EDPB's geolocation guidelines under purpose limitation.
B. AI Act's high-risk bans.
C. Data Act's fair access, but not GDPR.
D. NIS2 cybersecurity only.

Answer: A
Explanation: Location personal; Article 5(1)(b) limits to delivery, per 2026 EDPB geo-guidelines curbing secondary analytics. DPIA for real-time.

Question: 1475

In a scenario where a new automated decision-making system is introduced, which concern should a privacy impact assessment focus on?

A. Number of users accessing the company website
B. Marketing costs associated with the new system
C. System downtime during weekends
D. Potential bias and fairness issues impacting data subjects' rights

Answer: D

Explanation: Automated decision-making poses privacy risks related to fairness, bias, and transparency, which must be assessed during the PIA to safeguard individuals' rights.

Question: 1476

A data protection officer (DPO) is reviewing a company's data processing activities. Which of the following is a key responsibility of the DPO?

A. Conducting all data processing activities
B. Making final decisions on data breaches
C. Ensuring compliance with data protection laws
D. Approving marketing strategies

Answer: C

Explanation: A key responsibility of the DPO is to ensure compliance with data protection laws. This includes advising the organization on legal obligations and monitoring data processing activities to protect individuals' rights.

Question: 1477

A healthcare consortium in the EU is architecting a blockchain-based platform for sharing patient consent records across member states, where smart contracts automate data access based on predefined conditions. To comply with privacy by default under GDPR, the default configuration must limit processing to essential attributes only, such as hashed consent timestamps rather than full medical histories. During testing, the security audit reveals that optional fields for supplementary data could be inadvertently enabled. What benefit of applying Privacy by Design principles would most directly mitigate this by ensuring built-in data minimization from the protocol layer?

A. Stronger stakeholder trust
B. Reduced breach exposure
C. Enhanced regulatory compliance

D. Improved operational efficiency

Answer: B

Explanation: Applying Privacy by Design principles, particularly data minimization and privacy by default, significantly reduces exposure to breaches by limiting the volume and sensitivity of data processed in systems like blockchain platforms, where immutable ledgers amplify risks if excess data is included. In this scenario, configuring defaults to process only hashed essentials prevents unnecessary retention of medical histories, aligning with GDPR's emphasis on necessity and proportionality, thereby lowering the blast radius of potential compromises. This contrasts with compliance benefits, which are more procedural, or trust-building, which is relational, as the core advantage here is technical risk reduction through proactive safeguards, evidenced by lower incident rates in privacy-embedded architectures per industry benchmarks.

Question: 1478

A 2026 Finnish health app aggregates user-input symptom logs with wearables data under consent for epidemic modeling, shared pseudonymously with ECDC. A Helsinki user, post-modeling phase, requests the right to be forgotten for logs containing sensitive mental health entries, fearing stigma in future insurance applications. The app's retention is 5 years for research, with data in Azure EU zones. What balances the erasure request?

A. Erasure of identifiable logs, with model aggregates retained under Article 89 statistical safeguards if anonymized
B. Denial citing epidemic public interest exemption, offering restriction as alternative
C. Full erasure including model contributions, as consent revocation overrides research retention
D. Partial erasure of symptoms, keeping wearables for ongoing monitoring consent

Answer: A

Explanation: Article 17 GDPR mandates erasure on consent withdrawal for no longer necessary data, but Article 89 permits retention for scientific research with technical/organizational measures like anonymization ensuring aggregates are non-personal. Mental health logs as special category data (Article 9) heighten sensitivity, requiring erasure of raw entries, but model contributions can persist if irreversibly anonymized per 2026 ECDC guidelines. The app must erase identifiable instances across Azure, notify recipients like ECDC, and restrict processing

during verification, within one month. Public interest exemptions apply narrowly; stigma risks justify erasure over retention, with documentation for DPA audits.

Question: 1479

A data subject has requested the deletion of their personal data. Under what condition can the organization refuse this request according to GDPR?

A. If the data subject has not provided adequate identification
B. If the data is no longer relevant
C. If the data is needed for compliance with a legal obligation
D. If the data was obtained with explicit consent

Answer: C
Explanation: Organizations can refuse a data deletion request if the data is necessary for compliance with a legal obligation. GDPR allows for certain exceptions where data must be retained despite a deletion request, particularly for legal compliance.

Question: 1480

An energy utility in Austria, a public authority, initiates GDPR alignment. Which early activity is compulsory in their compliance sequence?

A. Encrypting all smart meter data immediately
B. Conducting public awareness campaigns on energy data
C. Limiting data sharing with contractors
D. Appointing a Data Protection Officer as mandated for public bodies

Answer: D
Explanation: As a public authority, appointing a Data Protection Officer (Article 37(1)(a)) is compulsory early in compliance. The DPO oversees all activities (records, DPIAs for smart meters); campaigns, encryption (Article 32), and limiting sharing (Article 28) follow DPO advice—appointment enables structured alignment.

Question: 1481

A 2026 sustainable fashion app uses EU users' Instagram eco-posts to score carbon footprints for green badges, sharing scores with affiliates. If posts reveal lifestyles, what joint controllership duty under GDPR ensures rights flow-through?

A. Separate consents for scoring
B. Unified privacy policy only
C. Independent DPIAs per entity
D. Public agreement detailing each party's obligations

Answer: D
Explanation: Article 26(2) obliges joint controllers' transparent public agreement on respective duties, including direct rights exercise to data subjects (e.g., objection cascades). For lifestyle-derived scores, this delineates app vs. affiliate roles; 2026's affiliate marketing crackdowns by BEUC demand published AAAs (Accountability Agreements), with user portals for seamless rights, preventing fragmented compliance and unified liability.

Question: 1482

An organization receives a request from an individual to delete their personal data. Under which circumstance might the organization refuse this request?

A. The data is required for compliance with a legal obligation
B. The individual has previously consented to the data processing
C. The data is no longer necessary for the purpose it was collected
D. The individual has not provided sufficient identification

Answer: A
Explanation: An organization may refuse to delete personal data if it is necessary for compliance with a legal obligation, such as retaining financial records for tax purposes. This reflects the

balance between individual rights and legal requirements.

Question: 1483

During the rollout of a cloud-based HR analytics tool for a global bank, the vendor's API endpoints are set to transmit employee performance metrics, including geolocation tags from mobile check-ins, to centralized servers unless manually adjusted. The bank's DPO mandates a redesign incorporating end-to-end encryption and automated purging after 30 days. This adjustment exemplifies which of the seven Privacy by Design principles, ensuring that privacy protections are inseparable from core functionalities like predictive staffing models?

A. End-to-end security – full lifecycle protection
B. Privacy as the default setting
C. Positive-sum – not zero-sum
D. Hiding complexity – user-friendly simplicity

Answer: A
Explanation: The principle of end-to-end security in Privacy by Design mandates comprehensive protection across the entire data lifecycle, from collection via mobile check-ins to analysis and disposal, integrating measures like encryption and timed purging to safeguard against interception or persistence risks. In this HR tool scenario, embedding these into the API ensures that privacy is not an add-on but a foundational element, complying with GDPR's security of processing requirements under Article 32 and preventing scenarios where geolocation data could enable unauthorized surveillance. This principle extends beyond default settings, which focus on initial configurations, or user-friendly simplicity, which addresses interface design, by enforcing holistic, continuous security that maintains data integrity throughout operations.

Question: 1484

In a 2026 multinational pharmaceutical trial conducted across EU member states, researchers collect biometric data from participants for efficacy testing of a new drug. Midway, the sponsor requests repurposing anonymized subsets for AI-driven predictive modeling on disease outbreaks under public health mandates. Which action ensures compliance with GDPR's purpose limitation

principle?

A. Anonymize the data fully and process it without further notification, as public health exemptions override purpose constraints.
B. Retain the data in the original database but apply pseudonymization for the new modeling, relying on legitimate interests balancing test.
C. Obtain explicit consent from all participants for the secondary AI modeling use, documenting it in updated privacy notices.
D. Proceed with repurposing after a Data Protection Impact Assessment confirms low risk and compatibility with initial health research purposes.

Answer: D
Explanation: The GDPR's purpose limitation principle under Article 5(1)(b) requires personal data to be collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner. However, further processing for archiving in the public interest, scientific, or historical research, or statistical purposes is not considered incompatible per Article 89(1), provided appropriate safeguards like pseudonymization are implemented. In this scenario, repurposing for AI-driven public health modeling aligns as compatible scientific research. A DPIA under Article 35 is mandatory for high-risk processing involving new technologies like AI, to assess necessity, proportionality, and risks to rights and freedoms. This ensures the secondary purpose remains linked to the original health research without requiring new consent, as long as compatibility is demonstrated and safeguards mitigate re-identification risks. Anonymization would remove GDPR applicability entirely, but the scenario specifies anonymized subsets, implying residual risks necessitating a DPIA. Explicit consent is not required for compatible research purposes, and legitimate interests (Article 6(1)(f)) are less suitable here due to the public interest nature.

Question: 1485

In a scenario where a 2026 podcast network monetizes EU listener pauses via acoustic fingerprinting for ad insertions, fingerprints are deemed personal data. What processor agreement clause is critical for the controller?

A. Sub-processor approval notifications

B. Assistance in DPIA consultations
C. All of the above
D. Confidentiality and return/destruction duties

Answer: C
Explanation: Article 28(3) mandates DPA clauses covering sub-processing, security/confidentiality, and controller assistance (including DPIAs per Article 35(2)), plus data return/deletion. For fingerprinting, this ensures vendors like Shazam-like services align with GDPR; 2026's audio ad tech evolves with mandatory audit rights, enabling controllers to verify compliance and mitigate indirect breaches through chained accountability.

Question: 1486

An insurance broker in Belgium experiences a ransomware attack exposing client claims data. Post-incident review highlights weak organizational safeguards. What is the key importance of data protection for the organization in this crisis recovery phase?

A. Lowering tax liabilities via privacy investments
B. Achieving certification badges for marketing materials
C. Simplifying annual reporting requirements
D. Preventing operational disruption and ensuring business continuity through resilient practices

Answer: D
Explanation: In a ransomware attack exposing claims data, the key importance of data protection is preventing operational disruption and ensuring business continuity through resilient practices. GDPR requires integrity and confidentiality (Article 5(1)(f)), with measures like encryption and backups (Article 32). Strong protection minimizes downtime, avoids breach notification chaos (Articles 33-34), and supports recovery—critical for an insurance broker where trust is core. This outweighs marketing, tax, or reporting benefits in a crisis where non-resilience could lead to lost clients and further fines.

Question: 1487

In Slovenian court, data subject claims compensation for distress from exposed sensitive data; controller argues no intent—what GDPR right under Chapter III enables effective remedy against denial?

A. Prior consultation appeal
B. Judicial remedy access
C. Right to compensation pursuit
D. Legitimate interest override

Answer: B
Explanation: Judicial remedy under Article 79 allows courts to hear claims independently of supervisory complaints, enforcing rights like compensation for breaches. Compensation is outcome.

Question: 1488

In a 2026 Belgian retail chain's loyalty program, purchase scans with CCTV link to cards, inferring religious practices from halal buys. Data fuels personalized ads. What special category is inferred, and what fairness principle is risked?

A. Religious beliefs as special, risking discriminatory profiling.
B. Practices as standard consumer data, fairness via opt-outs.
C. Scans as non-personal footage, no fairness issue.
D. Buys as contractual, exempting risks.

Answer: A
Explanation: Inferred religious beliefs (Article 9(1)(d)) are special category, processable for contract (Article 9(2)(c)) but risking fairness (Article 5(1)(a)) through biased ads. DPIA (Article 35) and equality impact assessments are needed, aligning with 2026 EDPB retail profiling opinions emphasizing non-discrimination.

Question: 1489

Scenario: Amid 2026 geopolitical tensions affecting supply chains, a Dutch logistics conglomerate with affiliates in Turkey and Russia is enhancing its BCR to cover just-in-time inventory data of EU suppliers, including personal contact details for emergency rerouting. The updated EDPB procedure requires demonstrating BCR deployment across the group. What key implementation aspect must the conglomerate's BCR include to ensure binding application to non-EU affiliates?

A. Signed undertakings or equivalent binding commitments from each group entity, integrated into employment and inter-company contracts
B. Annual certification by an external auditor without entity-specific sign-offs
C. Public disclosure of BCR on the conglomerate's global website for transparency
D. Voluntary adoption clauses allowing affiliates to opt into BCR for specific data types only

Answer: A
Explanation: BCR require formal, binding commitments from every group entity (including non-EU ones) to comply, typically via signed undertakings, amendments to articles of association, or incorporation into employment contracts and intra-group agreements, ensuring enforceability as per Article 47(2)(a) GDPR and the 2024 EDPB Recommendations. For the Dutch conglomerate's logistics data flows, this means Turkish and Russian affiliates must explicitly commit to GDPR standards (e.g., security under Article 32), with sanctions for non-compliance, verifiable during the streamlined 2026 approval process involving lead authority (Dutch AP) and EDPB opinion. Voluntary opt-ins undermine universality, public disclosure alone lacks legal force, and external audits supplement but do not replace entity bindings. This structure supports resilient supply chain processing by embedding BCR into operational contracts, as emphasized in recent EDPB guidance on deployment monitoring.

Question: 1490

A controller receives simultaneous identical breaches from two different processors on the same day. The 72-hour clock:

A. Runs separately for each breach
B. Starts only for the larger breach
C. Is combined into one notification

D. Is paused until root cause analysis

Answer: A
Explanation: Each breach is assessed and notified separately if distinct incidents, even if similar nature. Combining is possible only if truly the same incident.

Question: 1491

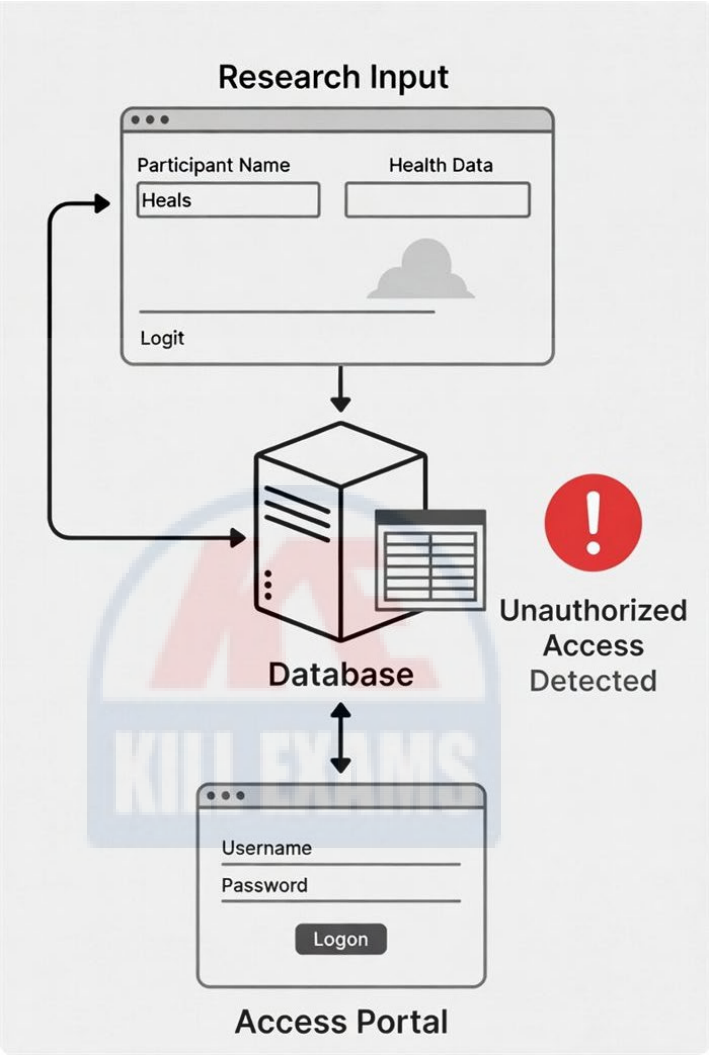
Consider a 2026 marketing firm employing zero-party data collection via interactive quizzes on a website, where EU participants voluntarily share preferences for personalized newsletter content, but the firm repurposes this data for third-party sales without updating its privacy notice. Which GDPR right is most directly infringed, and what remedial step must the firm implement?

A. Right to erasure; conduct a full data deletion audit
B. Right to object; provide an automated opt-out mechanism
C. Right to rectification; verify data accuracy quarterly
D. Right to access; disclose processing logs annually

Answer: B
Explanation: The right to object under GDPR Article 21(2) applies specifically to processing for direct marketing, including profiling, allowing individuals to withdraw consent at any time with immediate effect. In this scenario, repurposing zero-party data for sales without notice violates purpose limitation (Article 5(1)(b)) and mandates an easy opt-out tool, such as a one-click unsubscribe in emails or website dashboards, to align with ePrivacy Directive synergies and avoid enforcement actions like those seen in recent CNIL fines for opaque data flows.

Question: 1492

A university’s research database suffers a security incident, with its data flow depicted in a diagram.



According to GDPR, how should this incident be classified?

A. Technical error
B. User error
C. Security incident
D. Data breach

Answer: D
Explanation: Article 4(12) of the GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. The unauthorized access detected in Component 2 constitutes a data breach, as it involves personal data (participant names and health data). A security incident is broader and may not involve personal data, while technical or user errors are not GDPR-specific classifications.

Question: 1493

A financial services firm conducting a privacy audit discovers inconsistent consent withdrawal mechanisms in its cross-border transaction app after a recent data subject complaint. What is the primary purpose of initiating a full horizontal privacy audit across the app's end-to-end data lifecycle in response?

A. Benchmark audit findings against ISO 27001 security controls exclusively
B. Generate billing reports for audit-related consulting fees
C. Demonstrate compliance verification through independent process tracking
D. Update marketing materials highlighting audit completion badges

Answer: C
Explanation: The purpose of a privacy audit in PDPF context is to independently verify organizational compliance with data protection obligations by tracking processes holistically from data collection to deletion; horizontal audits follow a specific process end-to-end, ideal for app consent issues spanning frontend capture to backend revocation. This differs from vertical audits on single functions and supports ongoing governance. Audit plans include scope, objectives, methodology, and evidence requirements.

Question: 1494

A Bulgarian bank specifies "risk management" for transaction logs but extends to customer segmentation. What characterizes proper specification?

A. General industry norms
B. Detailed, foreseeable uses
C. Retrospective validation
D. Minimal disclosure

Answer: B
Explanation: Proper specification details uses like fraud detection, not broad risk, ensuring foreseeability and lawfulness (Article 5(1)(b)). Bulgarian CPC verifies via privacy notices.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, 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.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.