PassQueen
a.k.a dumpsqueen.com

Certified Information Privacy Manager (CIPM)

IAPP CIPM

Version Demo

Total Demo Questions: 31

Total Premium Questions: 312

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Privacy Program Governance	31
Topic 2, Privacy Program Framework	61
Topic 3, Privacy Operational Life Cycle	138
Topic 4, Privacy Program Assessment and Improvement	73
Topic 5, Mix Questions	9
Total	312

QUESTION NO: 1

Which of the following is NOT recommended for effective Identity Access Management?

A. Demographics.

B. Unique user IDs.

C. User responsibility.

D. Credentials (e.g.. password).

ANSWER: A

Explanation:

Demographics. is the correct selection because demographic characteristics describe broad population traits rather than providing a dependable, account-specific basis for controlling access. Attributes such as age, gender, location, or income may be personal data and may be relevant to a business process, but they do not establish that a particular person requesting access is the authorized account holder. Effective identity and access management depends on reliably associating an individual or service with a distinct identity, authenticating that identity through suitable credentials or authenticators, and authorizing only the access needed for the approved purpose.

Using demographic information as an access-control mechanism would also create privacy and governance concerns. Such data can be inaccurate, change over time, be shared by many people, and may constitute sensitive or regulated information depending on the jurisdiction and context. An IAM program should therefore minimize its use of personal information and use identity attributes only when they are necessary, accurate, and appropriately governed. NIST's digital identity guidance distinguishes identity proofing, authentication, and federation, emphasizing evidence and authenticators rather than population characteristics for assurance decisions. NIST's access-control guidance likewise frames authorization around identified subjects, accounts, and permissions. See NIST Digital Identity Guidelines and NIST Guide to Attribute Based Access Control.

QUESTION NO: 2

SCENARIO

Please use the following to answer the next QUESTION:

Martin BriseÃ±o is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, BriseÃ±o decided to change the hotelâ€™s on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading BriseÃ±o to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of BriseÃ±oâ€™s program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the userâ€™s name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHTâ€™s profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e- learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training

programâ€™s systems and records remained in Pacific Suitesâ€™ digital archives, un-accessed and unused. BriseÃ±o and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Trainingâ€™s customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

In the Information Technology engineers had originally set the default for customer credit card information to â€œDo Not Save,â€ this action would have been in line with what concept?

A. Use limitation

B. Privacy by Design

C. Harm minimization

D. Reactive risk management

ANSWER: B

Explanation:

Privacy by Design is correct because it requires privacy protections to be embedded proactively into a system's architecture and operating defaults, rather than relying on an individual to locate and select a more protective setting. One of the foundational Privacy by Design principles is "privacy as the default setting": individuals should receive the strongest practical privacy protection automatically, without needing to take affirmative action.

Setting credit-card information to "Do Not Save" by default would reduce the volume of sensitive payment data retained in the training platform. A participant could still provide card details to complete a particular transaction, but the system would not persist those details for later use unless a deliberate, appropriate choice and supporting controls justified retention. This implements data minimization at the design stage and reduces the amount of information exposed if systems are compromised or retained beyond their useful life. It also reflects the proactive, lifecycle-oriented approach central to Privacy by Design. The Privacy by Design framework identifies "privacy as the default setting" as a core principle: Foundational Principles of Privacy by Design. The IAPP also describes Privacy by Design as integrating privacy into systems and business practices from the outset: IAPP Privacy by Design overview.

QUESTION NO: 3

If your organization has a recurring issue with colleagues not reporting personal data breaches, all of the following are advisable to do EXCEPT?

A. Carry out a root cause analysis on each breach to understand why the incident happened.

B. Communicate to everyone that breaches must be reported and how they should be reported.

C. Provide role-specific training to areas where breaches are happening so they are more aware.

D. Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.

ANSWER: D

Explanation:

“Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.” is the exception because a phishing simulation primarily evaluates awareness of suspicious messages and users’ ability to identify a common security threat. Although phishing exercises can be a useful component of a wider security-awareness program, they do not directly identify why colleagues fail to recognize, escalate, or report suspected personal data breaches through the organization’s incident-management process. A recurring failure to report requires measures targeted at reporting behavior: clear and repeated communications on what constitutes an incident, how to report it, and the expectation to report promptly; role-relevant training where patterns indicate a knowledge or process gap; and root-cause analysis to identify cultural, procedural, technical, or accountability barriers. These actions support an effective breach-response capability by ensuring that potential incidents reach the appropriate team quickly enough to assess risk, contain harm, and meet any applicable notification deadlines. The UK Information Commissioner’s Office emphasizes having breach-detection, investigation, and internal-reporting procedures, as well as staff awareness, in place. See the ICO guidance on personal data breaches and the ICO personal data breaches guide.

QUESTION NO: 4

MULTI-SELECT â€“ Select 3

A multinational manufacturing company is considering outsourcing its HR data processing to a third-party vendor based in a country with less strict data protection laws. The company has a large database of employee information, including personal and sensitive data such as national ID numbers, medical information and employment contracts. The third-party vendor has a reputation for providing cost-effective services and has assured the company that it can handle the data securely.

The data protection officer (DPO) should ensure which of the following contractual requirements are included in the agreement with the third-party vendor?

A. How a breach would be handled.

B. How the vendor is insured.

C. How data transfers take place.

D. How appropriate security will be maintained.

E. How the cost of doing business will be reduced.

ANSWER: C

Explanation:

How data transfers take place is the best single answer because the scenario expressly involves outsourcing employee data to a vendor located in another country whose legal protections are described as less strict. The DPO must ensure that the agreement identifies a lawful transfer mechanism and establishes enforceable safeguards for the international disclosure of personal data. Under the GDPR’s transfer framework, a controller may transfer personal data outside the European Economic Area only where the applicable conditions in Chapter V are met. Depending on the destination and circumstances, this may include an adequacy decision, appropriate safeguards such as the European Commission’s Standard Contractual Clauses, or a narrowly applicable derogation. The contract should also clearly allocate transfer-related responsibilities and ensure that the vendor can meet the required safeguards throughout the processing relationship. This is particularly important for HR records because they contain high-risk information, including identifiers and health information. The European Commission explains the role of Standard Contractual Clauses in legitimizing transfers to third countries at its SCC guidance page. The governing GDPR transfer requirements are set out in Chapter V of Regulation (EU) 2016/679.

QUESTION NO: 5

SCENARIO

Please use the following to answer the next QUESTION:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.

Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What does this example best illustrate about training requirements for privacy protection?

A. Training needs must be weighed against financial costs.

B. Training on local laws must be implemented for all personnel.

C. Training must be repeated frequently to respond to new legislation.

D. Training must include assessments to verify that the material is mastered.

ANSWER: B

Explanation:

Training on local laws must be implemented for all personnel. Privacy training must enable employees and managers to recognize that a practice permissible, familiar, or tolerated in one jurisdiction may be subject to materially different requirements in another. Here, the manager applied video surveillance for employee-performance monitoring after arriving in Ireland, despite the cameras having been designated for facility security. That change in use raises core local privacy-law issues, including purpose limitation, transparency to employees, proportionality, and the safeguards required when monitoring workers.

Effective privacy-management training is therefore not limited to general statements about collecting or protecting data. It should be role- and jurisdiction-specific: managers who can access, repurpose, or make employment decisions from surveillance footage need practical instruction on the local rules governing those activities and on when to seek privacy or legal review. This allows the organization to operationalize its privacy commitments consistently across locations and to avoid relying on assumptions formed under another country's practices.

The Irish Data Protection Commission's guidance emphasizes that CCTV processing must have a clear lawful purpose and that use of CCTV in workplaces requires particular care and transparency. See the Irish Data Protection Commission CCTV guidance. The GDPR's accountability principle also requires organizations to implement appropriate measures demonstrating compliance, including staff awareness measures where appropriate; see GDPR Article 5 and Article 24.

QUESTION NO: 6

Which of the following practices best ensures the continuous assessment of program performance within the operational life cycle?

A. Completing third-party audits by subject matter experts.

B. Prioritizing ongoing improvement efforts.

C. Evaluating emerging risks every 24 months.

D. Allocating training costs in favor of the privacy and security teams.

ANSWER: B

Explanation:

Prioritizing ongoing improvement efforts best ensures continuous assessment because it makes performance review, measurement, corrective action, and refinement recurring operational activities rather than isolated events. A mature privacy program uses feedback from monitoring, metrics, incidents, stakeholder input, regulatory developments, and operational outcomes to identify where controls or processes need adjustment. The resulting improvements are then incorporated into the program and assessed again, creating a sustained improvement cycle throughout the program's operational life.

This approach aligns with the CIPM emphasis on managing privacy as an enduring organizational program, including measuring performance and evolving the program as organizational risks, processing activities, and legal obligations change. Continuous improvement also reflects established management-system practice: organizations should evaluate performance and use those results to improve the system on an ongoing basis. Embedding this discipline in routine governance enables the program to remain effective, accountable, and responsive over time. See the IAPP's CIPM certification overview and NIST's Privacy Framework, which describes privacy risk management as a continuous, adaptable process.

QUESTION NO: 7

SCENARIO

Please use the following to answer the next QUESTION:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:

1. Send an enrollment invitation to everyone the day after the contract is signed.

2. Enroll someone with just their first name and the last-4 of their national identifier.

3. Monitor each enrollee's credit for two years from the date of enrollment.

4. Send a monthly email with their credit rating and offers for credit-related services at market rates.

5. Charge your company 20% of the cost of any credit restoration.

You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

Which of the following elements of the incident did you adequately determine?

A. The nature of the data elements impacted

B. The likelihood the incident may lead to harm

C. The likelihood that the information is accessible and usable

D. The number of individuals whose information was affected

ANSWER: D

Explanation:

The number of individuals whose information was affected was adequately determined. The facts establish a definite population: the company sent surveys for exactly 2,000 individuals to the vendor, the planned notification concerned all 2,000 affected individuals, and enrollment invitations were ultimately sent to those same 2,000 people. This repeated, consistent count supports documenting the incident's affected-population figure as 2,000 rather than relying on an estimate.

Establishing the number of affected people is a core incident-assessment and notification-record element. For example, the GDPR's breach-notification requirements call for the controller, where possible, to state the approximate number of data subjects concerned. The European Commission summarizes this obligation in its guidance on personal-data-breach notification: European Commission data protection guidance. Similarly, the U.S. Department of Health and Human Services breach-notification materials require covered entities to maintain and report breach information, including the number of individuals affected: HHS Breach Notification Rule.

Here, the organization had a concrete count before issuing notices and retained that count through its mitigation process. That is sufficient to conclude that the incident's affected-individual total was determined.

QUESTION NO: 8

Your marketing team wants to know why they need a check box for their SMS opt-in. You explain it is part of the consumer's right to?

A. Request correction.

B. Raise complaints.

C. Have access.

D. Be informed.

ANSWER: D

Explanation:

Be informed. is correct because a meaningful SMS marketing opt-in must be presented transparently, so an individual can understand what they are agreeing to before taking an affirmative action. The consumer-rights principle of being informed requires an organization to provide clear, accessible information about the collection and use of personal data, including the purpose of the processing and relevant communications practices. In this setting, the opt-in mechanism should be

accompanied by concise disclosure explaining that the person is electing to receive SMS marketing messages, who will send them, and material terms such as message frequency or applicable charges where relevant.

The checkbox is not merely an internal marketing control. It supports a transparent consumer interaction by making the proposed communication visible and enabling the consumer to make an informed decision before enrollment. It also creates a record that the organization can use to demonstrate that the individual took a deliberate affirmative step. This reflects the transparency information expected when personal data is collected and used, as described in Article 13 of the GDPR: GDPR official text. For SMS marketing, clear disclosure and affirmative consent are also central to the FCC's consumer-protection framework: FCC rules for calls and texts.

QUESTION NO: 9

MULTI-SELECT (Select 3 of 5)

(A multinational manufacturing company is considering outsourcing its HR data processing to a third-party vendor based in a country with less strict data protection laws… The DPO should ensure which of the following contractual requirements are included in the agreement with the third-party vendor?)

A. How a breach would be handled.

B. How the vendor is insured.

C. How data transfers take place.

D. How appropriate security will be maintained

E. How the cost of doing business will be reduced.

ANSWER: A C D

Explanation:

"How a breach would be handled," "How data transfers take place," and "How appropriate security will be maintained" are essential contractual requirements for a processor handling HR information internationally. A processor agreement must establish the processor's duties to assist the controller with security and personal-data-breach obligations. In practical terms, this should define incident escalation points, notification timeframes, cooperation in investigation and containment, preservation of relevant evidence, and support for any required notifications to authorities or affected individuals.

The agreement must also specify appropriate technical and organisational measures for the risk presented by the processing. For HR data, these measures commonly address access management, confidentiality commitments, encryption or other protections, logging, resilience, testing, and controls over any sub-processors. The controller must be able to demonstrate that the processor provides sufficient guarantees.

Because the vendor is located in a country with less stringent protections, the contract must document the lawful international-transfer mechanism and associated safeguards. Depending on the circumstances, this can include adequacy regulations, standard contractual clauses, or another permitted mechanism, together with restrictions and controls for onward transfers. These provisions create accountability and help ensure protection continues when data is processed outside the originating jurisdiction. See GDPR, particularly Articles 28, 32, 33, and 44–49 and the European Commission's standard contractual clauses guidance.

QUESTION NO: 10

A company is acquiring a smaller business that holds customer data in several legacy systems. What should the privacy manager do first to identify material privacy risks associated with the acquisition?

A. Conduct privacy due diligence on the target company's data practices.

B. Merge the companies' customer databases immediately after signing the acquisition agreement.

C. Publish a new enterprise privacy notice before reviewing the target's systems.

D. Require all target-company employees to complete privacy training before evaluating the transaction.

ANSWER: A

Explanation:

Conduct privacy due diligence on the target company's data practices. is correct because the acquiring company needs to understand what personal data the target holds, how it was collected and used, where it is stored, which vendors receive it, what incidents or complaints have occurred, and which legal or contractual obligations apply. This information allows the company to identify risks before the transaction closes and to plan remediation and integration activities.

Privacy due diligence is an important element of transaction risk management. It can reveal undisclosed security incidents, inaccurate notices, excessive retention, unsupported marketing practices, deficient vendor contracts, or data uses that cannot lawfully continue after acquisition. A post-closing data inventory may still be necessary, but it does not replace early review of the target's privacy posture. See the NIST Privacy Framework for governance and privacy-risk-management context.

QUESTION NO: 11

When implementing an organization's privacy program, what right should be granted to the data subject?

A. To have their data amended or erased if errors are found.

B. To limit or refuse the disclosure of their data for any reason.

C. To provide feedback regarding an organization's privacy policy.

D. To verify that an organization uses the highest level of privacy protection available.

ANSWER: A

Explanation:

To have their data amended or erased if errors are found is the appropriate data-subject right because an effective privacy program must provide a way for individuals to maintain the accuracy of personal information held about them. Data quality and individual participation are foundational privacy principles: individuals should be able to challenge inaccurate, incomplete, or outdated information and have the organization correct it. Where retaining erroneous information is no longer justified or correction is not appropriate, deletion may be necessary, subject to applicable legal, contractual, and records-retention obligations.

This operationally requires the organization to establish a documented request process, authenticate the requester, locate relevant records, assess the request, correct or erase data where required, and communicate the outcome within the applicable legal timeframe. These procedures support trustworthy processing and reduce the risk that decisions are made using incorrect personal data. For example, the GDPR expressly provides a right to rectification of inaccurate personal data in Article 16 and a right to erasure in specified circumstances in Article 17. See the GDPR Article 16 text and the UK ICO guidance on the right to rectification.

QUESTION NO: 12

In a sample metric template, what does "target" mean?

A. The suggested volume of data to collect

B. The percentage of completion

C. The threshold for a satisfactory rating

D. The frequency at which the data is sampled

ANSWER: C

Explanation:

“The threshold for a satisfactory rating” is correct because a target states the performance level that the organization intends to attain or regards as acceptable for a metric. In privacy-program measurement, a metric converts an operational or governance objective into something observable, while the target supplies the benchmark against which the reported result is evaluated. For example, if a program measures the percentage of data-subject requests completed within the required period, its target might be 95% or higher. The resulting measurement can then be assessed as meeting, exceeding, or falling short of the desired standard, allowing privacy leadership to prioritize corrective action and demonstrate accountability. This use of targets supports the CIPM emphasis on establishing, operating, and monitoring a privacy program through meaningful performance measures. IAPP describes the CIPM as focusing on the practical management of privacy programs, including measuring and reporting program performance; see the IAPP CIPM certification overview. This approach also aligns with the accountability principle, under which organizations should implement and be able to demonstrate appropriate privacy governance measures; see the ICO Accountability Framework.

QUESTION NO: 13

(Which of the following should be your first step when conducting an internal privacy audit focused on identifying cross-border data transfers in cloud environments?)

A. Map the data and the locations where it is processed.

B. Review the data inventory.

C. Enable encryption of the data in transit by default.

D. Review the list of the cloud providers and their location.

ANSWER: A

Explanation:

Map the data and the locations where it is processed. is the appropriate first step because a cross-border-transfer audit must first establish the actual path of personal data through the cloud environment. This means identifying the relevant datasets, the cloud services and subprocessors involved, and each location where the data is accessed, stored, backed up, or otherwise processed. The resulting data-flow map establishes whether a transfer occurs and identifies the parties and jurisdictions involved, creating the factual basis for assessing applicable transfer requirements and safeguards.

This approach is consistent with accountability practices: records of processing must capture relevant processing details, and transfer assessments require an organization to understand the particular transfer and its destination. In cloud environments, processing may occur across several regions and may include remote support, resilience copies, and provider subprocessors, so a location-aware map is essential before evaluating contracts, transfer tools, or technical controls. The European Data Protection Board explains that a transfer analysis begins by identifying the processing and disclosure/access arrangement at issue in its Guidelines 05/2021. The GDPR’s recordkeeping requirements also support documenting processing activities and, where applicable, transfers to third countries; see Article 30 GDPR.

QUESTION NO: 14

A Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) are conducted during what phase of a System Development Life Cycle (SDLC)?

A. Testing.

B. Design.

C. Deployment.

D. Maintenance.

ANSWER: B

Explanation:

Design. is correct because privacy assessments are intended to identify and address privacy risks before the system's architecture, data flows, requirements, vendors, and controls are finalized. Conducting a Privacy Threshold Analysis, Privacy Impact Assessment, or Data Protection Impact Assessment during design makes privacy an engineering and governance input rather than a late-stage compliance check. The assessment process documents what personal data will be processed, the purposes and legal or organizational basis for processing, affected individuals, recipients, retention, security measures, and anticipated risks. Its findings can then drive design decisions such as data minimization, role-based access, encryption, logging, retention controls, user notices, and mechanisms for individual rights. This supports the privacy-by-design approach expected of an effective privacy management program. A DPIA in particular must be completed early enough for the organization to implement measures that mitigate identified high risks before processing begins. Assessments should also be revisited when material changes occur, but their primary SDLC placement is the design stage, where changes are practical and substantially less costly. See the European Data Protection Board guidance on DPIAs and NIST Security Considerations in the System Development Life Cycle.

QUESTION NO: 15

Under the General Data Protection Regulation (GDPR), international data transfer is allowed using the mechanisms in all of the following scenarios EXCEPT between companies who?

A. Are part of the same group of enterprise using approved Binding Corporate Rules (BCRs).

B. Have signed up to the EU Standard Contractual Clauses.

C. Have put in place a binding confidentiality agreement.

D. Have put in place an approved code of conduct.

ANSWER: C

Explanation:

"Have put in place a binding confidentiality agreement" is the correct answer because confidentiality terms alone are not a GDPR Chapter V transfer mechanism. A confidentiality agreement can establish an important security and secrecy obligation between contracting parties, but it does not by itself provide the safeguards and enforceable data-subject rights required for transfers of personal data to a third country or international organisation in the absence of an adequacy decision. GDPR Article 46 requires the controller or processor to provide appropriate safeguards and to ensure that enforceable data-subject rights and effective legal remedies are available. The safeguards expressly recognized include standard data-protection clauses, binding corporate rules, and approved codes of conduct accompanied by binding and enforceable commitments of the recipient outside the EU/EEA. In practice, a transfer mechanism also requires an assessment of the particular transfer and, where necessary, supplementary measures to ensure protection essentially equivalent to that guaranteed in the EU. Confidentiality may be included as a contractual or technical-organisational safeguard, but cannot independently authorize the international transfer. See GDPR, especially Articles 44–46 and the European Commission's guidance on standard contractual clauses.

QUESTION NO: 16

(MULTI-SELECT – Which of the following are technical data controls?)

A. Firewall.

B. Encryption.

C. Data minimization.

D. Pseudonymization.

E. Multifactor authentication.

ANSWER: A B D E

Explanation:

Firewall, encryption, pseudonymization, and multifactor authentication are technical data controls because they are implemented through technology to protect data or systems that process data. A firewall applies network rules to restrict unauthorized connections and limit exposure of systems and data. Encryption uses cryptography to protect the confidentiality of data at rest and in transit, including when storage media or communications are accessed without authorization. Multifactor authentication is a technical access-control mechanism that strengthens identity verification before granting access to data or applications.

Pseudonymization is also appropriately classified as a technical data control when it is applied using systems or processes that replace direct identifiers with pseudonyms and keep the additional information needed for reidentification separately protected. It reduces the linkability of data to an individual and is expressly recognized by the GDPR as a security measure relevant to risk-based protection. The European Data Protection Board further describes pseudonymization as a technical and organizational measure that can support data-protection compliance. These controls can be combined in a defense-in-depth approach: identity controls restrict access, firewalls constrain network exposure, encryption protects data content, and pseudonymization reduces identifiability in processing datasets. See GDPR Article 32 and the EDPB Guidelines on Pseudonymisation.

QUESTION NO: 17

MULTI-SELECT – Select 3

A multinational manufacturing company is considering outsourcing its HR data processing to a third-party vendor based in a country with less strict data protection laws. The company has a large database of employee information, including personal and sensitive data such as national ID numbers, medical information and employment contracts. The third-party vendor has a reputation for providing cost-effective services and has assured the company that it can handle the data securely.

The data protection officer (DPO) should ensure which of the following contractual requirements are included in the agreement with the third-party vendor?

A. How a breach would be handled.

B. How the vendor is insured.

C. How data transfers take place.

D. How appropriate security will be maintained.

E. How the cost of doing business will be reduced.

ANSWER: A C D

Explanation:

How a breach would be handled, **How data transfers take place**, and **How appropriate security will be maintained** are core processor-contract requirements for this arrangement. A written agreement with a processor should require the vendor to assist the controller with security incidents, including prompt notification and the information needed for the controller to assess, contain, document, and, where necessary, report a personal data breach. This is especially important because the data set includes sensitive employee health information and identifiers.

The agreement must also establish a lawful mechanism and documented conditions for transferring employee data to the vendor's country. Where the destination does not benefit from an adequacy decision, the parties must use an appropriate transfer safeguard, such as standard contractual clauses, and assess whether supplementary measures are necessary. Finally, the contract should specify appropriate technical and organizational measures, proportionate to the risks posed by the processing. These measures may include access controls, encryption, confidentiality commitments, logging, resilience, testing, and controls for authorized sub-processors. GDPR Article 28 expressly requires processor contracts to address security and assistance with breach obligations, while Chapter V governs international transfers. See GDPR Article 28 and GDPR Chapter V.

QUESTION NO: 18

A "right to erasure" request could be rejected if the processing of personal data is for?

A. An outdated original purpose.

B. Compliance with legal obligation.

C. The offer of information society services.

D. The establishment of personal legal claims.

ANSWER: B

Explanation:

“Compliance with legal obligation.” is correct because the GDPR right to erasure is not absolute. Article 17(3)(b) expressly permits a controller to refuse erasure where processing remains necessary for compliance with a legal obligation under EU or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority. In practice, this commonly applies where retention is required by tax, accounting, employment, anti-money-laundering, or similar statutory recordkeeping duties. The controller should identify the applicable legal obligation, retain only the data necessary to meet it, and respect the relevant mandatory retention period. It should also respond to the data subject’s request transparently, explaining that erasure cannot be completed to the extent the information must be retained for that obligation. Once the legal retention requirement ends, the organization should erase or anonymize the data unless another valid basis and retention need applies. This exception reflects the GDPR’s balance between individuals’ control over personal data and organizations’ binding legal duties. See GDPR, Article 17(3)(b) and the European Commission’s overview of data-subject rights.

QUESTION NO: 19

SCENARIO

Please use the following lo answer the next question:

You are the privacy manager within the privacy office of a National Forest Parks and Recreation Department. While having lunch with a colleague from the IT division, you learn that the IT director has put out a request for proposal (RFP) which calls for a system that collects the personal data of park attendees.

You consult with a few other colleagues in IT and learn that the RFP is worded such that it leaves it to the vendors to demonstrate what information they would collect from people who enter parks anywhere in the country, either in a vehicle or on foot. A partial list of the information collected includes:

â€¢ personal identifiers such as name, address, age, gender;

â€¢ vehicle registration information:

â€¢ facial images of park attendees;

â€¢ health information (e.g.. physical disabilities, use of mobility devices)

The stated purpose of the RFP is to:

"Improve the National Forest. Parks, and Recreation Department's ability to track and monitor service usage thereby Increasing the robustness of our customer data and to improve service offerings."

Companies have already started submitting proposals for software solutions that address these information gathering practices. There is only one week left before the RFP closes.

The IT department has put together an RFP evaluation team but no one from the privacy office has been a Dart of the RFP ud to this point. This occurred deposite the factâ€¦.

Which of the following is the least important privacy consideration associated with assessing data when implementing a large-scale project like this?

A. Standardization of privacy safeguards on a national scale.

B. Classification of the types of personal information collected by the system

C. Identifying operational risks associated with data storage, access and disposal.

D. Third-party vendor assessment to determine how well privacy practices of vendors align with your organization's practices.

ANSWER: A

Explanation:

Standardization of privacy safeguards on a national scale. is the least important consideration specifically when assessing the data involved in this proposed system. A data assessment should first establish what personal information will be collected, why each data element is necessary, how sensitive data such as facial images and health information will be handled, and the risks arising across the information life cycle. These foundational activities enable the privacy office to determine whether the proposed collection is proportionate to the stated purpose and to identify appropriate controls before procurement decisions are finalized.

National consistency may become valuable when designing and operating a department-wide privacy program, particularly to support uniform implementation and governance across parks. However, it is a broader program-design objective rather than a core, immediate activity for assessing the data practices and privacy risks of a proposed collection system. The NIST Privacy Framework identifies data processing, governance, and risk assessment as central elements of privacy risk management: NIST Privacy Framework. Similarly, privacy-by-design practices call for privacy requirements and risk analysis to be integrated early in project and procurement lifecycles: IAPP: Privacy by Design.