DUMPSARENA

DSCI certified Privacy Professional (DCPP)

DSCI DCPP-01

Version Demo

Total Demo Questions: 18

Total Premium Questions: 242

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Privacy Fundamentals	32
Topic 2, Privacy Principles and Frameworks	37
Topic 3, Privacy Laws and Regulations	120
Topic 4, Privacy Governance	18
Topic 5, Privacy Operations	21
Topic 6, Privacy Engineering	14
Total	242

QUESTION NO: 1

Company A collects and stores information from people X & Y on behalf of company B. Which of the following statements are true?

A. A is the data controller since it collects data directly from X & Y

B. B is the data controller while A is the sub processor as B has outsourced the data collection and processing to A

C. B is the data controller that uses A as data processor to collect and process data of data subjects X and Y

D. Both A & B are data controllers since both need to maintain highest principles of data protection

ANSWER: C

Explanation:

"B is the data controller that uses A as data processor to collect and process data of data subjects X and Y" is correct because the determining factor is not which organisation physically collects or stores the personal data; it is which organisation determines the purposes and means of the processing. In this scenario, Company B engages Company A to perform collection and storage on B's behalf. B therefore decides why the personal data of X and Y is needed and directs the relevant processing activity, making B the controller. Company A processes the information under B's authority and for B's instructed purposes, which is the defining role of a processor. The controller must ensure that its processor provides sufficient guarantees for appropriate technical and organisational safeguards and that processing is governed by a suitable data-processing arrangement. This controller–processor allocation supports accountability by placing responsibility for the processing objectives and lawful basis with the organisation that makes the substantive decisions about the data use. See the GDPR definitions in Article 4 of Regulation (EU) 2016/679 and the European Data Protection Board's Guidelines on the concepts of controller and processor.

QUESTION NO: 2

Technological advancement is inevitable and the speed of change is exponential. In such a scenario, which of the following statement is not true for defining the relationship between privacy protection and technology advancement, both at individual and corporate levels?

A. Maintaining privacy is difficult with emerging platforms and services

B. Maintaining privacy is difficult, as exercising complete control over personal information in online environment is an uphill task

C. Technology advancements and privacy protection are independent concepts that are not related

D. Maintaining privacy in cyberspace becomes easier with proper use of tools and technologies

ANSWER: C

Explanation:

Technology advancements and privacy protection are independent concepts that are not related is the statement that is not true. Technology directly shapes how personal data are collected, inferred, transmitted, stored, shared, secured, and deleted. New platforms, connected devices, cloud services, analytics, and artificial intelligence can create new processing purposes and privacy risks; equally, technical measures can support privacy through access controls, encryption, data minimisation, pseudonymisation, and privacy-by-design practices. Therefore, privacy cannot be treated as separate from technological advancement at either an individual or organisational level. Responsible innovation requires organisations to assess privacy implications throughout a technology lifecycle, rather than considering privacy only after a system has been deployed. This relationship is reflected in the privacy-by-design principle, which calls for privacy to be embedded into the design of technologies and business practices. It is also consistent with the OECD Privacy Guidelines, which recognise that evolving technologies affect the collection and use of personal data and require appropriate safeguards. See the Privacy by Design guidance and the OECD Privacy Framework.

QUESTION NO: 3

ABC company is a large US based IT Company that provides a range of services to its clients. The company had developed a cloud based application providing end-to-end services for the medical industry. The application had three modules for:

-Patients

-Hospitals and Doctors

-Insurance and Pharmaceutical companies

Each of the modules was designed to be integrated with others depending on user's choice. For example, a patient could choose to share his/her medical history with his/her doctor (for medical advice) as well as insurance companies (for claims).

The application requires that all registered users of the application read and acknowledge the privacy policy. Additionally, users are required to identify the purpose for which they are providing any personal data in any of the modules. For example, a patient providing his/her medical history and current symptoms can select 'Medical Advice' as the purpose for the data being provided.

Few months ago, company launched new services in the applications namely, Business Analytics, Group Consultations, Insurance Policy purchase, and Medical Trials Management. The new services used all existing data collected over the years from users. The Company's clients/users are based only in three geographical locations - United States, European Union and India. Additionally, to facilitate better performance of its application, the company established one datacenter each in US, Germany and India for its operations. Each of the datacenter provides the following: -US Datacenter - Storage of data for US based users only

-Germany Datacenter - Storage of data for EU based users only

-India Datacenter - Storage of data for India based users and alternate site for US and Germany Datacenters (used as part of global load balancing) -Services of a cloud service provider are leveraged in US as a Disaster Recovery (DR) site for Indian Datacenter

Recently, the company's Application Support Desk has started receiving user complaints related to unsolicited communications.

These complaints have warranted a review of company's privacy policies as well as practices.

What all will be the directly or indirectly applicable laws on the data stored on US cloud service provider? i. HIPAA

ii. German Data Protection Act iii. IT(Amendments) Act, 2008 Sec 43A iv. None of the above as data protection laws are not applicable on Cloud Service Providers

A. iv

B. i and ii

C. i, ii and iii

D. ii and iii

ANSWER: C

Explanation:

i, ii and iii is correct because the US cloud service provider is the disaster-recovery environment for the Indian data centre, and that Indian centre also acts as an alternate processing site for the US and German data centres. Consequently, the DR environment can contain or process health and personal data originating from all three regions; legal accountability follows the data, the processing role, and the relevant territorial scope, rather than the physical location of the backup alone.

For US health information, HIPAA can apply where the application operator is a covered entity or business associate and the cloud provider creates, receives, maintains, or transmits protected health information on its behalf. HIPAA expressly contemplates business-associate arrangements for such processing; see the HHS HIPAA Privacy Rule resources.

German/EU personal data handled through the German data-centre and its alternate or DR processing remains subject to the applicable German and EU data-protection framework despite an overseas transfer. The territorial and processing scope of EU data-protection obligations is set out in Article 3 of the GDPR.

For Indian-origin data, Section 43A of India's Information Technology Act establishes liability where a body corporate handling sensitive personal data is negligent in implementing reasonable security practices. This responsibility is not removed by using a foreign cloud DR provider.

QUESTION NO: 4

Which of the following privacy legislations is synonymous with "Data Handlers"?

A. Federal Data Protection Act, Germany (BDSG)

B. South Korea's Personal Information Protection Act

C. Digital Privacy Act, 2015

D. Child online protection Act, 1998

ANSWER: B

Explanation:

South Korea's Personal Information Protection Act is correct because its privacy framework uses the term "personal information handler," a role that corresponds to the general concept of a data handler. Under the Act, a personal information handler is an individual who processes personal information under the direction and supervision of a personal information controller. This terminology distinguishes the organization or person deciding how personal information is processed—the controller—from personnel who actually handle or process the information in the course of performing assigned duties. The term is therefore central to South Korean privacy governance, particularly for defining responsibilities associated with the handling, security, and appropriate processing of personal information. The distinction supports accountability by requiring those handling information to act within the controller's instructions and protective measures. The official English legal search portal maintained by the Korean government provides the text and current status of the Personal Information Protection Act: Korean Law Information Center—Personal Information Protection Act. Further privacy-law guidance and regulatory information are available from South Korea's Personal Information Protection Commission at pipc.go.kr.

QUESTION NO: 5

According to RTI Act, under which conditions can a government department refuse to release information?

A. National security adversely affected by such information

B. This information is detrimental to the stability of the ruling party in government

C. Detrimental effect on the public image of government agencies

D. In the absence of a public interest, such information may adversely impact the privacy of its officials

ANSWER: A D

Explanation:

"National security adversely affected by such information" is correct because section 8(1)(a) of India's Right to Information Act, 2005 exempts information whose disclosure would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific, or economic interests of the State, relations with a foreign State, or could lead to incitement of an offence. This permits a public authority to withhold such protected information when the statutory threshold is met.

"In the absence of a public interest, such information may adversely impact the privacy of its officials" is also correct in principle. Section 8(1)(j) protects personal information where disclosure has no relationship to a public activity or interest, or would cause an unwarranted invasion of an individual's privacy. The provision also requires disclosure where the competent authority is satisfied that a larger public interest justifies it. The privacy exemption can apply to personal information relating to public officials, but it is not a blanket protection for all information concerning them. These exemptions must be applied consistently with the Act's disclosure framework and the particular facts of the request. See section 8 of the Right to Information Act, 2005 and the Department of Personnel and Training RTI portal.

QUESTION NO: 6

Which of the following privacy regulation advocates de-identification of personal information?

A. EU Data Protection Directive

B. Canada's PIPEDA

C. Australia's ANPP

D. IT Act of India

ANSWER: C

Explanation:

Australia's ANPP is correct because the former Australian National Privacy Principles expressly required an organisation to take reasonable steps to destroy or *permanently de-identify* personal information when it is no longer needed for a purpose permitted under the principles. This places de-identification directly within the information life-cycle and disposal obligation: once an organisation no longer has a legitimate need to retain identifiable information, it should ensure that individuals can no longer be identified from the retained material. Permanent de-identification is therefore a privacy-protective alternative to retaining identifiable records and reduces the risk that unnecessary personal information can be accessed, disclosed, or misused.

The ANPP framework was contained in the Privacy Act 1988 before being replaced by the Australian Privacy Principles. Its treatment of de-identification remains relevant to understanding the privacy-management principle tested here. The current Australian Privacy Principles preserve the same practical approach: APP 11.2 requires reasonable steps to destroy or de-identify personal information that is no longer needed, subject to legal retention requirements. See the Australian Government's Privacy Act 1988 and the Office of the Australian Information Commissioner's guidance on APP 11: security of personal information.

QUESTION NO: 7

Which among the following is the Canadian privacy law?

A. COPPA

B. PIPEDA

C. HIPAA

D. IT Act of Canada

ANSWER: B

Explanation:

PIPEDA is the correct answer. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal private-sector privacy law. It establishes rules for how organizations collect, use, and disclose personal information in the course of commercial activities, and it grants individuals rights to access and request correction of their personal information. PIPEDA is built around fair information principles, including accountability, identifying purposes, consent, limiting collection, safeguards, openness, and individual access. It applies across Canada to federally regulated organizations and to many commercial activities, although some provinces have substantially similar private-sector privacy legislation that applies within their jurisdictions. Privacy professionals should recognize PIPEDA as a foundational Canadian privacy framework and understand that its requirements are administered by the Office of the Privacy Commissioner of Canada. The official legislation is available through the Justice Laws website, while practical guidance and regulatory information are provided by the Office of the Privacy Commissioner of Canada.

QUESTION NO: 8

Which of the following applies to the HIPAA Omnibus rule as of 2013?

A. Federal Health Bodies only

B. Business Associates only

C. Covered Entities only

ANSWER: B C

Explanation:

The HIPAA Omnibus Rule applies to both “Business Associates only” and “Covered Entities only,” meaning that each of these organization types is within the rule’s scope. The final Omnibus Rule, published in January 2013, implemented statutory amendments under the HITECH Act and made business associates directly accountable for compliance with applicable HIPAA Privacy Rule and Security Rule requirements. A business associate is a person or organization that performs specified functions or activities involving protected health information on behalf of a covered entity.

Covered entities—including health plans, health care clearinghouses, and health care providers that conduct covered electronic transactions—also remain subject to the HIPAA Rules. The Omnibus Rule updated obligations for covered entities, including requirements associated with privacy practices, uses and disclosures of protected health information, and business-associate arrangements. Consequently, privacy professionals should recognize the 2013 rule as extending direct HIPAA accountability to business associates while continuing to govern covered entities. HHS summarizes the final rule and its applicability at HHS: Final Omnibus Rule. Definitions and the respective roles of covered entities and business associates are available at HHS: Covered Entities and Business Associates.

QUESTION NO: 9

Data Protection Impact Assessment requirement, under GDPR is triggered if the organization is engaged in which of the following activities?

A. Processing on a large scale of special categories of data

B. Processing on a large scale of personal data relating to criminal convictions and offences

C. Systematic monitoring of a publicly accessible area on a large scale

D. All the above

ANSWER: D

Explanation:

“All the above” is correct because each stated activity, when performed at the specified scale, is explicitly identified by the GDPR as a type of processing likely to result in a high risk to individuals’ rights and freedoms. A Data Protection Impact Assessment is therefore required before the processing begins. Article 35 requires controllers to assess the necessity and proportionality of the proposed processing, identify risks to data subjects, and document measures that will address those risks. In particular, the GDPR names large-scale processing of special-category data, large-scale processing of data relating to criminal convictions and offences, and large-scale systematic monitoring of a publicly accessible area as circumstances requiring a DPIA. These activities can create substantial privacy impacts because they involve sensitive information, potentially serious consequences for affected people, or pervasive observation in places accessible to the public. The assessment must be performed early enough to shape the design of the processing and ensure appropriate safeguards are built in. See GDPR Article 35 at EUR-Lex and the European Data Protection Board’s DPIA guidelines.

QUESTION NO: 10

What of the following is a lawful basis under Article 6 of the General Data Protection Regulation, 2016?

A. Legitimate Interest

B. Consent

C. Legal Obligation

D. Vital Interest

E. Performance of Contract

ANSWER: A B C D E

Explanation:

Article 6(1) of the GDPR establishes the conditions under which processing of personal data is lawful. **Legitimate Interest** is a lawful basis where processing is necessary for the controller's or a third party's legitimate interests, provided those interests are not overridden by the data subject's rights and freedoms. **Consent** is lawful when the data subject has given valid, freely given, specific, informed, and unambiguous consent to the relevant processing. **Legal Obligation** applies when processing is necessary for the controller to comply with a legal obligation imposed by applicable law.

Vital Interest permits necessary processing to protect the vital interests of an individual or another natural person, such as an urgent life-or-death situation. **Performance of Contract** applies where processing is necessary to perform a contract with the data subject or to take steps at that person's request before entering into a contract. Controllers must select the basis that genuinely reflects the purpose and necessity of the processing before it begins, and document that decision as part of accountability. The authoritative wording appears in GDPR Article 6 on EUR-Lex; practical guidance is also available from the ICO's lawful-basis guidance.

QUESTION NO: 11

XYZ is a successful startup that acquired a respectable size & scale of operations in last 3 years, handling business process services for small & medium scale enterprises, largely in US & Europe. They are at the stage of closing a deal with a new banking client and working out the details of privacy related obligations in contract. Ensuring effective enforcement of which of the below listed privacy principles is client's accountability, even after outsourcing its loan approval process to XYZ?

I. Notice

II. Choice and Consent

III. Collection Limitation

IV. Use Limitation

V. Access and Correction

VI. Security

VII. Disclosure to third Party

Please select the correct set of principles from below listed options:

A. None of the above, since they are outsourcing the work to XYZ who will carry the liability going forward

B. All except V and VI

C. All except III

D. All of the above listed privacy principles

ANSWER: D

Explanation:

All of the above listed privacy principles is correct because outsourcing a loan-approval process does not transfer the banking client's accountability for personal-data processing. The client determines the purpose and essential means of processing customer information and therefore remains responsible for ensuring that its service provider processes that information in accordance with the client's privacy obligations. This responsibility covers providing appropriate notice, obtaining and honoring valid choices or consent where required, limiting collection to what is necessary, restricting use to

authorized purposes, enabling data-subject access and correction, applying appropriate security safeguards, and controlling onward disclosure to third parties.

The outsourcing contract is a key accountability mechanism: it should document the processor's instructions, confidentiality duties, security requirements, controls for sub-processors and onward transfers, assistance with individual-rights requests, incident notification, audit or assurance rights, and deletion or return of data at the end of the engagement. These contractual and governance measures enable the client to demonstrate that the principles are effectively enforced throughout the processing lifecycle. The EU GDPR expressly requires a controller to use processors providing sufficient guarantees and to bind them by a compliant processing contract; see GDPR, Article 28. The OECD Privacy Guidelines likewise identify collection limitation, use limitation, security safeguards, openness, individual participation, and accountability as core privacy principles; see OECD Privacy Guidelines.

QUESTION NO: 12

From the following list, select the element (elements) that comprise APEC's cross border privacy rules system:

A. recognition/acceptance by APEC members

B. dispute resolution and enforcement

C. self-assessment

D. compliance review

ANSWER: A B C D

Explanation:

APEC's Cross-Border Privacy Rules system is designed as an accountability-based mechanism for organizations transferring personal information across participating economies. It begins with *self-assessment*, through which an organization assesses its own privacy policies and practices against the applicable CBPR program requirements. That assessment is then subject to *compliance review* by an APEC-recognized Accountability Agent. Once the review requirements are met, *recognition/acceptance by APEC members* enables the organization's certification to be recognized within participating economies. The system also requires effective *dispute resolution and enforcement*: certified organizations must provide mechanisms for handling complaints, cooperate with the Accountability Agent, and remain subject to appropriate enforcement consequences if they fail to meet their commitments. These elements operate together to make the system more than a voluntary privacy statement; they create a structured process for demonstrating, validating, recognizing, and maintaining cross-border privacy accountability. APEC's published CBPR program requirements describe self-assessment, accountability-agent review, recognition, and ongoing compliance and enforcement as core operational features. See the APEC CBPR System Program Requirements and the APEC CBPR System overview.

QUESTION NO: 13

What conditions apply in India for a company to transfer sensitive personal information (SPI) to another Indian company or individual, or to a person residing in any other country?

A. A transfer may occur only where the data subject gives their consent or when it is necessary to perform a lawful contract

B. In India, the Chief Information Commissioner must approve the transfer of information

C. Data may be transferred to companies that adhere to the same level of data protection that is required by Indian law

D. Taking permission from the ministry of electronics and information technology is necessary for information transfer.

ANSWER: A C

Explanation:

Under Rule 7 of India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, a body corporate may transfer sensitive personal data or information to another body

corporate or person, whether located in India or abroad, only when specified safeguards and grounds are present. The recipient must maintain the same level of data protection that the transferring body corporate is required to maintain under those Rules. This makes the protection standard applicable to the recipient a core condition of a permitted transfer, rather than limiting the rule solely to international recipients.

In addition, the transfer must be necessary for the performance of a lawful contract between the body corporate and the information provider, or the information provider must have consented to the transfer. These are alternative legal grounds under the Rule. Accordingly, “A transfer may occur only where the data subject gives their consent or when it is necessary to perform a lawful contract” and “Data may be transferred to companies that adhere to the same level of data protection that is required by Indian law” accurately state the applicable conditions. See Rule 7 in the IT SPDI Rules, 2011 and the Information Technology Act resources published by MeitY.

QUESTION NO: 14

Privacy enhancing tools aim to allow users to take one or more of the following actions related to their personal data that is sent to, and used by online service providers, merchants or other users: i. Increase control over their personal data

ii. Choose whether to use services anonymously or not iii. Obtain informed consent about sharing their personal data iv. Opt-out of behavioral advertising or any other use of data

Please select correct option from below:

A. Only i

B. Only i and ii

C. All

D. Only ii

ANSWER: C

Explanation:

“All” is correct because privacy-enhancing tools and technologies are designed to give individuals practical agency over how their personal data is collected, disclosed, processed, and reused in digital interactions. This can include tools that provide privacy settings and preference controls, enable data minimisation or pseudonymous/anonymous use where feasible, and present meaningful notice and consent choices before personal information is shared. Such tools can also support the exercise of choices relating to secondary uses of data, including controls for interest-based or behavioural advertising.

Privacy is not achieved solely through an organisational policy; effective privacy management also requires mechanisms that allow people to understand and act on their choices. For example, consent-management interfaces can record and communicate an individual’s sharing preferences, while advertising preference tools can let individuals limit personalised advertising based on their activity. Privacy-enhancing measures therefore cover each listed outcome: enhanced personal-data control, the ability to use a service with reduced identifiability where supported, informed consent for sharing, and opt-out choices for behavioural advertising or other optional processing. This aligns with the privacy-by-design approach described by the UK Information Commissioner’s Office in its guidance on data protection by design and default and the consumer-choice framework described by the US Federal Trade Commission for behavioural advertising.

QUESTION NO: 15

APPI, the Act for the Protection of Personal Information, applies to:

A. Government entities using personal information

B. Personal Information about an individual that is used by a business

C. None of the above

ANSWER: B

Explanation:

Personal Information about an individual that is used by a business is the best answer because the APPI's core private-sector obligations apply when a business operator handles personal information in connection with its business activities. The Act regulates the collection, use, retention, disclosure, and safeguarding of information that can identify a living individual, including information that can be readily combined with other information to identify that person. In practical privacy-management terms, this means an organization must assess whether the information it handles is personal information and, if so, apply APPI requirements such as specifying and notifying or publicly announcing purposes of use, maintaining appropriate security controls, and managing third-party provision appropriately. The relevant regulated entity is generally described as a Personal Information Handling Business Operator, rather than the individual whose information is involved. APPI obligations can also apply to an overseas business operator when it handles personal information in relation to supplying goods or services to individuals in Japan. The Personal Information Protection Commission provides official information on Japan's personal-information protection framework at https://www.ppc.go.jp/en/. An English legal translation of the Act is available through Japanese Law Translation.

QUESTION NO: 16

As a privacy assessor, what would most likely be the first artifact you would ask for while assessing an organization which claims that it has implemented a privacy program?

A. Privacy risk management framework

B. Records of privacy specific training imparted to the employees handling personal information

C. Personal information management policy

D. Records of deployed privacy notices and statements

ANSWER: C

Explanation:

Personal information management policy is the most appropriate first artifact because it establishes the organization's formal, top-level commitment to privacy and defines the scope, principles, governance, accountability, and intended controls of its privacy program. An assessor needs this foundational document early to understand what the organization says it has implemented, which business units and processing activities are within scope, who owns privacy responsibilities, and which internal requirements or external obligations the program is designed to meet.

The policy provides the baseline against which supporting evidence can be assessed. It helps structure later assessment activities by identifying expected procedures, operational controls, training responsibilities, risk-management practices, notice requirements, and review mechanisms. It also demonstrates that privacy is governed through management-approved direction rather than only through isolated operational practices. A personal information management policy therefore gives the assessor a coherent view of the program's design before examining implementation records and evidence.

This approach aligns with the privacy-management-system model described in ISO/IEC 27701, which extends information-security management with privacy governance requirements. It is also consistent with DSCI's focus on organizational privacy capability and accountability; see DSCI.

QUESTION NO: 17

XYZ Inc of USA has setup a captive back office operations center in India. The captive is registered as a separate legal entity by the name XYZ India Private Limited and provides services only to XYZ Inc by catering its technology support needs. During the process of providing services, the Indian entity does not receive any customer information of the XYZ Inc. However, information such as financial information and biometric information etc. of the employees of XYZ India is shared with the XYZ Inc.

What necessary steps need to be taken before actual sharing of the aforesaid information happens?

1. Seek consent from the employees of XYZ India before sharing the information;

2. A lawful contract between the XYZ Inc and XYZ India regarding the terms of sharing and data protection measures to be taken, with the obligation on XYZ Inc of not sharing the received informationfurther without permission from Indian entity;

3. The XYZ Inc should agree to provide better or at-par level of data protection as prescribed in the IT (Amendment) Act, 2008;

4. The country in which the XYZ Inc is located should ensure better or same level of data protection as prescribed in the IT (Amendment) Act, 2008

A. 1 and 2

B. 1, 2 and 3

C. 2 and 3

D. 1 and 4

ANSWER: C

Explanation:

2 and 3 is the correct selection under the sensitive personal data and information transfer requirements addressed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Financial information and biometric information are sensitive personal data or information. Before XYZ India transfers such employee information to its US parent, the transfer arrangement should be governed by a lawful contract that sets out the processing purpose, confidentiality obligations, security controls, and restrictions on onward disclosure. This gives XYZ India a documented mechanism to ensure that the recipient handles the information only for the agreed business purpose and with appropriate safeguards.

In addition, the overseas recipient, XYZ Inc, must ensure the same level of data protection that XYZ India is required to maintain under the applicable Indian rules. The transfer standard focuses on the protection ensured by the recipient body corporate or person, rather than requiring a general finding that the recipient's country has an equivalent privacy regime. A written intra-group data-transfer agreement, supported by enforceable security and confidentiality commitments, is therefore central to demonstrating compliant handling of employees' sensitive information. See Rule 7 of the SPDI Rules, 2011 and the Information Technology Act, 2000.

QUESTION NO: 18

Which of the following instruments can be used for a legal data transfer when a company in the EU wishes to transfer data to Asian countries?

A. Framework for the Privacy Shield

B. Standard Contractual Clauses

C. Data processors must be certified by ISO 27001 under customized contracts

D. Binding Corporate Rules

ANSWER: B D

Explanation:

Standard Contractual Clauses and Binding Corporate Rules are recognised transfer mechanisms under Chapter V of the EU General Data Protection Regulation when personal data is transferred from the European Economic Area to a recipient in a third country that is not covered by a European Commission adequacy decision. Standard Contractual Clauses are contractual terms adopted by the European Commission that impose enforceable data-protection obligations on the data exporter and importer. They are commonly used for transfers between independent controllers, between controllers and processors, and in certain processor-to-processor arrangements. The parties must also assess whether the law and practice of the destination country could affect the effectiveness of the clauses and implement supplementary measures where necessary. Binding Corporate Rules provide an alternative for multinational groups making regular intra-group international transfers. They are legally binding internal privacy rules that must be approved by the competent supervisory authorities and must give data subjects enforceable rights. Both mechanisms require accountability, documented assessments, and

appropriate technical and organisational protections for the transferred data. The European Commission describes the current SCC mechanism at its Standard Contractual Clauses page, and the European Data Protection Board explains the requirements for Binding Corporate Rules.