CIPP/CN 笔记 题目在最后

一、考试内容大纲（核心五大领域）

1.中国隐私与数据保护法律框架

核心法律：《个人信息保护法》（PIPL）、《数据安全法》（DSL）、《网络安全法》（CSL）

相关法规：《个人信息出境标准合同办法》《数据出境安全评估办法》等部门规章与司法解释

2.监管机构与执法机制

国家互联网信息办公室（网信办）等监管机构的职责、执法权限与处罚措施

行业监管要求（如金融、医疗、电信等重点行业的特殊规定）

3.数据主体权利

知情权、决定权、更正权、删除权、可携权等权利的内涵与实现路径

数据主体请求的处理流程与合规要求

4.数据处理合规实践

合法、正当、必要等核心原则的应用

数据最小化、目的限制、跨境数据传输规则（安全评估、标准合同、认证等）

5.隐私风险管理

隐私影响评估（PIA）、数据泄露应急响应、供应商隐私管理

隐私政策制定与合规审计

二、备考建议

1.《CIPP/CN Body of Knowledge and Exam Blueprint》，明确各领域权重与考点。

2. 重点研读 PIPL、DSL、CSL 三大核心法律，理解法条背后的立法意图与实践场景。

3.分析大厂合规事件（如数据泄露处罚、跨境传输案例），加深对知识点的理解。

4.关注中国隐私合规领域的最新动态（如网信办通报、法规更新），考试内容会反映最新政策变化。

5.增加行业洞察（**APP 监管、汽车行业、金融行业、人类遗传基因等 具体的法律对应的要求**）

6.再次汇总重点必考法律、法规、国家标准

（1）《中华人民共和国个人信息保护法》

关联：七大个人信息处理原则；个人信息与敏感个人信息的定义与区别；“告知-同意”核心规则及“单独同意”要求；个人信息主体的各项权利；个人信息跨境提供的三条路径；个人信息保护影响评估情形；法律责任与高额罚款。

（2）GB/T 35273《个人信息安全规范》

关联：将 PIPL 原则转化为具体操作要求；个人信息生命周期各环节的安全措施；去标识化与匿名化的具体技术和管理要求；个人信息安全事件处置。

（3）《数据出境安全评估办法》 《个人信息出境标准合同办法》

关联：数据出境的具体合规路径。重点掌握：何种情况下必须申报安全评估；何种情况下可订立标准合同；两种路径的适用条件、流程和材料要求。

（4）《中华人民共和国网络安全法》

关联：关键信息基础设施的保护要求；网络安全等级保护制度；网络运营者的安全义务。

（5）《中华人民共和国数据安全法》

关联：数据分类分级保护制度；重要数据的识别与保护；全流程数据安全管理制度。

（6）《儿童个人信息网络保护规定》

关联：处理儿童个人信息的特别严格规则；监护人明确同意的要求；专有的儿童隐私政策。

（7）《个人金融信息保护技术规范》

关联：金融信息的敏感程度分级；针对不同级别信息的技术；保护要求；金融业的典型合规**场景。** 场景题形式较多。（SCENARIO Please use the following to answer the next question:）

（8）《汽车数据安全管理若干规定（试行）》

关联：车内处理、匿名化处理、脱敏处理等原则；重要数据的出境要求；默认不收集等具体要求。 场景题形式较多。（SCENARIO Please use the following to answer the next question:）

（9）《互联网信息服务算法推荐管理规定》关联：算法透明和用户权益；关闭算法推荐的权利；禁止算法歧视、大数据杀熟等。

（10）《人脸识别技术应用安全管理规定（试行）》

关联：处理人脸信息的单独同意要求；非必要不采集原则； 不得利用人脸信息进行画像分析等禁止性行为。

（11）人口健康信息管理办法（试行）》

（12）《人类遗传资源管理条例》

（13）《中华人民共和国民法典》

关联：其**第四编第六章（第 1034-1039 条）** 是个人信息保护的民事权利基础。

考点：PIPL 中的处理原则（合法、正当、必要）在此有体现；明确自然人对个人信息享有**人格权益**。

（14）《中华人民共和国消费者权益保护法》

关联：其**第五章“消费者个人信息保护”**是早期对消费者领域个人信息的原则性规定。

考点：了解其被更专业、 更全面的 PIPL 所吸收和细化即可。

（15）《中华人民共和国未成年人保护法》

关联：其**网络保护**专章中有原则性规定。

考点：了解其与专门的《儿童个人信息网络保护规定》构成**一般法与特别法**的关系，后者规定更具体、优先适用。

（16）《刑法》及侵犯个人信息司法解释

关联：规定了**“侵犯公民个人信息罪”**的刑事责任，是个人信息保护最严厉的法律后果。

考点：了解该罪名的**大致入罪标准**（如信息类型、数量），知道出售、提供敏感个人信息量刑更重。**无需记忆具体数额。**

（17）《个人信用信息基础数据库管理暂行办法》

关联：是金融领域早期的专门规定，其核心精神已被《个人金融信息保护技术规范》等更新、更细化的标准所吸收。

考点：知道征信业务有特殊监管，目前由中国人民银行负责。

7. 考友分享汇总

中国个人信息保护概述部分

核心必背（必考）

核心三大法律

《网络安全法》：关键信息基础设施（CII）、等级保护（MLPS）

《数据安全法》：数据分类分级、安全责任、安全评估

《个人信息保护法》（PIPL）：个人信息保护核心法律

核心监管机构

网信办（CAC）：统筹监管、跨境数据、政策执法

公安部（MPS）：打击个人信息犯罪

工信部（MIIT）：互联网 / 电信行业监管

市场监管总局（SAMR）：消费者权益保护

央行（PBOC）：金融数据监管

高频考点

《民法典》：个人信息定义、处理原则、人格权保护

《刑法》：非法获取 / 出售 / 提供个人信息的刑事定罪标准

《消费者权益保护法》：消费者个人信息收集、使用限制

《未成年人保护法》：未成年人信息特殊保护、游戏服务时限

了解即可

《宪法》：隐私权、数据保护的根本依据

金融监管总局、国家卫健委、司法机构（最高法 / 最高检）次要职能

个人信息保护法（PIPL）部分【考试核心】

核心必背（100% 出题）

个人信息处理 7 大核心原则

合法性、正当必要性、诚信、透明、目的限制、数据最小化、数据安全

合法处理 6 大基础

同意、合同 / 人力必需、法定职责、公共健康应急、公共利益媒体报道、其他法律规定

个人信息主体 10 大权利

知情权、访问权、更正权、删除权、撤回同意权、限制 / 拒绝处理权、拒绝自动化决策权、解释权、申诉权、可携权

跨境数据传输 4 条路径

网信安全评估、个人信息保护认证、标准合同、国际条约 / 协议

PIA（个人信息保护影响评估）：处理敏感信息、自动化决策、委托 / 提供 / 公开信息、出境必做

问责核心：DPO（个人信息保护官）、数据处理记录、隐私政策 / 通知、数据泄露通知

高频考点

核心概念：个人信息、敏感个人信息、去标识化 vs 匿名化

处理者义务 + 大型互联网平台特殊义务

自动化决策：透明、公平、个人有权拒绝

执法处罚：刑事犯罪、行政罚款（最高 5000 万 / 年营收 5%）、公益诉讼

了解即可

地域 / 域外管辖细节、法律适用例外情形

数据质量、责任性原则次要表述

行业特定法规和合规部分：

核心必背（高频场景题）

儿童个人信息：《儿童个人信息网络保护规定》—— 监护人同意、专属保护

数据出境

《数据出境安全评估办法》：申报情形（重要数据、100 万人信息、累计 10 万 /1 万敏感信息）

《个人信息出境标准合同办法》：适用条件、签署要求

汽车数据：《汽车数据安全管理若干规定（试行）》—— 车内数据、出境限制、公示要求

人类遗传资源：中外合作项目出境需审批、安全评估

高频考点

个人金融信息：《个人金融信息保护技术规范》—— 分级保护、使用限制

算法推荐：《互联网信息服务算法推荐管理规定》—— 透明度、禁止大数据杀熟、公平性

就业场景：招聘非歧视、背景调查合法、 workplace 监控限制

互联网平台：禁止捆绑同意、数据最小化、电子营销合规

了解即可

刑事记录处理合规要求

生成式 AI 服务管理、医患保密细节

互联网平台社会责任报告等次要义务

三、考试基本信息

1.题型：90 道单选（75 道计分题 + 15 道不计分实验题，无法区分）

（1）常规的每题 ABCD 四个选项

（2）一段场景背景，描述一个具体的数据保护的情况，接下来的几道单选题都是在这个背景下进行的。（SCENARIO Please use the following to answer the next question: ）

2.时长：2.5h 含 15 分钟可选休息时间

3.评分标准：满分 500 分，300 分及以上即为通过

四、考题分享

Question#1　A medical institution in China is sorting out the diagnosis and treatment data of patients in the infectious disease department, and needs to classify the detailed medical records of AIDS patients in accordance with the national standard for health medical data security. According to GB/T 39725-2020 Information Security Technology - Guidelines for Health Medical Data Security, this type of data belongs to which level of health medical data?

A. Level 3 (Moderate sensitivity)

B. Level 4 (High sensitivity)

C. Level 5 (Highest sensitivity)

D. Level 2 (General sensitivity)

Answer: C

Explanation：According to GB/T 39725-2020 Information Security Technology - Guidelines for Health Medical Data Security, health medical data is classified into 5 levels based on its sensitivity level and the potential impact of a breach. Level 5 represents the highest sensitivity level and explicitly includes detailed diagnosis and treatment records of special diseases such as AIDS and sexually transmitted diseases (STDs).

Level 3 (Moderate sensitivity): Includes information such as outpatient queuing information.

Level 4 (High sensitivity): Includes general electronic medical records and hospitalization records.

Level 2 (General sensitivity): Includes anonymized epidemiological research data.

None of these levels meet the sensitivity threshold of AIDS-related data.

Regulatory Link

AIDS is classified as a Category B infectious disease under China's Law on the Prevention and Treatment of Infectious Diseases. Its diagnosis and treatment data is subject to the highest level of data governance due to its implications for personal dignity, privacy protection, and public health security.

(“What level of data are diseases like AIDS categorized into under a particular specification?")

Question #2 A Shanghai-based internet company intends to trade user portrait data (non-anonymized, involving basic personal information) through the Shanghai Data Exchange (SDE). According to the Shanghai Data Regulations and the Shanghai Data Exchange Trading Rules, which of the following steps is a mandatory prerequisite for the company to complete the data transaction?

A. Obtain separate explicit consent from each user whose portrait data is to be traded

B. Conduct a privacy impact assessment (PIA) and submit the report to the Shanghai Municipal Cyberspace Administration

C. Anonymize the user portrait data to eliminate all personal information identifiers

D. Register the transaction intention with the Shanghai Municipal Development and Reform Commission

Answer: A

Explanation：According to the Shanghai Data Regulations and SDE’s operational requirements, when trading personal information-related data through the exchange, data providers must ensure compliance with the Personal Information Protection Law (PIPL) and local regulations. Specifically, for non-anonymized user portrait data (which involves personal information), obtaining separate explicit consent from each data subject is a mandatory prerequisite for transaction eligibility. This is to protect data subjects’ right to decide on the use and disclosure of their personal information.

- B: A PIA is required for major data processing activities (e.g., large-scale personal information collection), but it is not a mandatory prerequisite for every data transaction at SDE. Only

transactions involving high-sensitivity data or large-scale personal information may require a PIA report submission.

- C: Anonymization is not mandatory for all data transactions at SDE. SDE allows transactions of de-identified personal information (not fully anonymized) as long as data subject consent is obtained and security measures are in place.

- D: The registration of data transaction intentions is handled by the Shanghai Data Exchange itself, not the Shanghai Municipal Development and Reform Commission. The latter is responsible for overall data development planning, not specific transaction registration.

Question #3

A medical institution in Shanghai plans to sell de-identified AIDS diagnosis data (in line with GB/T 39725-2020 Level 5 sensitivity) through the Shanghai Data Exchange. According to Shanghai's local data protection regulations and SDE's trading norms, which of the following statements about the data transaction is correct?

A. The data can be traded freely after de-identification, without additional security review by SDE

B. The medical institution must submit a data security assessment report to SDE before the transaction

C. The transaction price of the data can be determined independently by the medical institution without SDE supervision

D. The de-identified data can be re-identified by the buyer after the transaction, as it is no longer considered personal information

Answer: B

Explanation:Shanghai’s local data protection regulations (e.g., Shanghai Data Regulations) and the Shanghai Data Exchange Trading Rules clearly stipulate that for high-sensitivity health medical data (such as Level 5 AIDS diagnosis data, even after de-identification), data providers mustsubmit a data security assessment report to SDE before conducting transactions. This assessment aims to verify that the data de-identification process is compliant, the data source is legitimate, and there is no risk of re-identification or information leakage.

- A: High-sensitivity data cannot be traded freely even after de-identification. SDE conducts mandatory security reviews for transactions involving high-sensitivity data to ensure compliance with local and national regulations.
- C: The transaction price of data at SDE is determined through negotiation between the two parties, but it must be reported to SDE for filing and supervision. The medical institution cannot

determine the price independently without supervision to prevent irregular transactions.

- D: De-identified data that can be re-identified (even indirectly) is still regarded as personal information under Shanghai local regulations and PIPL. The buyer is prohibited from re-identifying the data after the transaction, and SDE imposes strict supervision on this behavior.

Question #4 A commercial bank in China needs to transfer important data and sensitive personal financial information collected from its domestic business to an overseas parent company. According to the Bank Insurance Institution Data Security Management Measures and national cross-border data transfer rules, which of the following statements is CORRECT?

A. The bank may directly transfer the data after obtaining verbal consent from data subjects.

B. The bank must conduct a data security assessment as required and bear full data security responsibility.

C. Cross-border transfer is fully prohibited for all financial important data and personal information.

D. The bank only needs to register the transfer with the local financial regulator without any security review.

Answer: B

Explanation：Under Article 36 of the Bank Insurance Institution Data Security Management Measures, when a bank or insurance institution provides important data and personal information collected and generated in domestic operations to an overseas recipient, it shall bear data security liability and complete a security assessment in accordance with national regulations.

A is wrong: Verbal consent is invalid; written or explicit separate consent is required for sensitive personal financial information.

C is wrong: Cross-border transfer is allowed if compliant with laws, security assessment, and proper safeguards.

D is wrong: Registration alone is insufficient; mandatory security assessment and compliance review are required.

Question #5

According to JR/T 0223-2021 Financial Data Security — Security Specification of Data Life Cycle, which rule applies to Level-5 core financial data generated within China?

A. It may be stored overseas with approval from the bank’s senior management.

B. It must be stored only within the territory of China.

C. It can be transferred overseas after simple encryption without further review.

D. It is exempt from all cross-border compliance requirements due to its low sensitivity.

Answer: B

Explanation:JR/T 0223-2021 clearly requires that Level-5 (highest sensitivity) financial data generated in China must be stored only within China. This is a mandatory local-storage rule for core financial data to safeguard financial security and personal rights.

A is wrong: Level-5 data cannot be stored overseas regardless of internal approval.

C is wrong: Cross-border transfer of Level-5 data is generally prohibited, not just encryption-based.

D is wrong: Level-5 is the highest sensitivity category and faces the strictest controls.

Question #6 A bank plans to collect and use customers' credit records and transaction history (categorized as sensitive personal financial information). Under the Personal Information Protection Law (PIPL) and financial industry protection guidelines, what is the legally required consent form?

A. Implied consent through continued use of banking services

B. Separate explicit consent given voluntarily by the data subject

C. Group consent covering all non-financial personal information

D. Consent obtained from the bank's compliance department on behalf of customers

Answer: B

Explanation：Sensitive personal financial information is a type of sensitive personal information under PIPL. Financial regulations and Personal Financial Information Protection Technical Specifications require that processing such information must be based on separate explicit consent from the data subject, not implied or bundled consent.

A is wrong: Implied consent does not meet the legal standard for sensitive personal financial information.

C is wrong: Group or bundled consent is invalid for sensitive financial data.

D is wrong: Consent must come from the data subject, not a third party or internal department.

Question #7 A company's HR director intends to check the criminal records of all current employees for internal management purposes. No position in the company is legally required to review criminal records. Under the Personal Information Protection Law

(PIPL) and relevant regulations on criminal record inquiry in China, which of the following statements is CORRECT?

A. The HR director may directly inquire about employees' criminal records through public security authorities.

B. The company may require employees to voluntarily submit their criminal records as a condition of employment.

C. Criminal records are sensitive personal information, and the company has no legal basis to inquire about them for general positions.

D. The company may collect criminal records if it informs employees in its privacy policy.

Answer: C

Explanation：Criminal records belong to sensitive personal information under the PIPL. In China, criminal record inquiries by employers are only allowed for legally prescribed positions (such as civil servants, teachers, police, security personnel, and certain financial practitioners). For ordinary positions, employers, including HR directors, do not have the legal right to inquire about or collect employees' criminal records, even with notice or consent.

A is wrong: Public security authorities will not accept unauthorized inquiries from ordinary companies.

B is wrong: Forcing submission of criminal records for general roles violates personal information protection rules.

D is wrong: Notice alone does not provide a legal basis for collecting criminal records.

Question #8 A bank hires a new employee for a position that by law requires a clean criminal record. Which of the following best describes the legitimate scope of the employer’s criminal record check under Chinese data protection rules?

A. The employer may check all criminal and administrative penalty records of the applicant.

B. The employer may only inquire about criminal records related to the position’s legal requirements.

C. The employer may share the criminal record information with all HR and department managers.

D. The employer may retain the criminal record permanently after employment.

Answer: B

Explanation：Even for positions that legally permit criminal record checks, the employer must follow the principles of minimization and necessity. It may only inquire about criminal records relevant to the legal requirements of the position, not all records.

A is wrong: Administrative penalties are not criminal records and are out of scope.

C is wrong: Criminal records must be strictly confidential and limited to authorized personnel only.

D is wrong: Criminal record information must be deleted or destroyed when no longer necessary.

Question #9 An automaker designs an in-car voice assistant that processes driver commands to control vehicle functions. According to China’s automotive data protection rules, which of the following practices BEST complies with the in-vehicle processing principle?

A. Transmit all voice data to the cloud server for processing by default

B. Process voice commands inside the vehicle and only transmit data outside when necessary with driver’s explicit consent

C. Store all voice data in the cloud for 7 years for product improvement

D. Share voice data with third-party service providers without driver notification

Answer: B

Explanation：The in-vehicle processing principle (Article 6 of the Provisions on Automotive Data Security Management (Trial Implementation)) requires that automotive data should be processed inside the vehicle unless it is absolutely necessary to transmit it outside. For in-car voice assistants, processing commands within the vehicle is the baseline compliance approach. When external transmission is required (e.g., for advanced features), it must be limited to necessary cases and supported by the driver’s explicit consent.

A is wrong: Default cloud transmission violates the in-vehicle processing principle and the "default non-collection" requirement.

C is wrong: Indefinite cloud storage contradicts the principle of data minimization and necessity; retention should be limited to the time required for specific purposes.

D is wrong: Sharing data with third parties without notification or consent directly violates the Personal Information Protection Law (PIPL) and automotive data regulations.

Question #10　A smart car manufacturer plans to transmit driving behavior data (including location and speed) to its overseas R&D center for product optimization. Under China’s automotive data

protection framework, which condition is NOT required for legal cross-border data transfer?

A. Conduct a data security assessment if the data qualifies as "important data"

B. Ensure the data is desensitized to remove direct or indirect personal identifiers

C. Obtain separate, explicit consent from vehicle owners for cross-border transfer

D. Process all driving behavior data inside the vehicle without any external transmission

Answer: D

Explanation：While the in-vehicle processing principle encourages on-board data handling, it does not impose an absolute ban on external transmission when there is a legitimate purpose and proper authorization. For cross-border transfer of automotive data, Chinese regulations require:

Security assessment: Mandatory for important data (e.g., precise location, driving trajectory) before cross-border transfer

Desensitization: Personal information should be anonymized or de-identified when transmitted outside the vehicle/China

Explicit consent: Separate, clear consent from data subjects is required for cross-border transfer of personal information, as per the PIPL

Option D is incorrect because it misrepresents the in-vehicle processing principle as an absolute prohibition on external data transmission, which is not the case under Chinese law.

Question #11 Which of the following is the superior law of the Data Security Law of the People's Republic of China?

A. Constitution of the People's Republic of China

B. Cybersecurity Law of the People's Republic of China

C. Personal Information Protection Law of the People's Republic of China

D. Civil Code of the People's Republic of China

Answer: A

Explanation: The Constitution is the fundamental law of China and the supreme superior law of all national laws, so it is the superior law of the Data Security Law.

Question #12 The Data Security Law of the People's Republic of China is mainly formulated in accordance with which of the following laws?

A. Personal Information Protection Law

B. Constitution of the People's Republic of China

C. Consumer Rights Protection Law

D. Anti-Monopoly Law

Answer: B

Explanation: The Constitution is the fundamental legal basis for enacting all laws in China, and the Data Security Law is formulated in accordance with the Constitution.

Question #13 According to the Cybersecurity Law of the People's Republic of China, what is the minimum mandatory retention period for network logs involving personal information?

A. 3 months

B. 6 months

C. 12 months

D. 24 months

Answer: B

Explanation: Pursuant to Article 21 of the Cybersecurity Law of the People's Republic of China, network operators shall retain relevant network logs for not less than six months in accordance with relevant provisions.

Question #14 According to Appendix B of GB/T 35273-2020 Information security technology — Personal information security specification, which of the following items is NOT personal sensitive information?

A. Ethnicity

B. Religious belief

C. Browsing page history

D. Biometric information

Answer: C

Explanation: According to Appendix B of GB/T 35273-2020, ethnicity, religious belief and biometric information are listed as personal sensitive information, while browsing page history is not classified as personal sensitive information.

Question #15 According to Appendix B of GB/T 35273-2020 Information security technology — Personal information security specification, which of the following statements is CORRECT?

A. Ethnicity is not personal sensitive information

B. Browsing page history is personal sensitive information

C. Ethnicity is personal sensitive information

D. Both ethnicity and browsing page history are personal sensitive information

Answer: C

Explanation: According to Appendix B of GB/T 35273-2020, ethnicity is defined as personal sensitive information, and browsing page history does not belong to personal sensitive information.

Question #16 According to GB/T 35273-2020 and Chinese personal information protection laws, which of the following constitutes a true anonymization measure?

A. Pseudonymization (using pseudonyms)

B. Ordinary hashing processing

C. Irreversible processing that makes data unable to identify any individual

D. Partial data masking

Answer: C

Explanation: True anonymization means personal information is processed to be non-identifiable to a specific natural person and irreversible; pseudonymization and hashing are de-identification measures, not anonymization.

Question #17 According to GB/T 35273-2020 (released before the Personal Information Protection Law), what type of consent is required for processing personal sensitive information?

A. General bundled consent

B. Implied consent

C. Separate and explicit consent

D. Oral consent

Answer: C

Explanation: Before the Personal Information Protection Law came into force, GB/T 35273-2020 clearly required that processing personal sensitive information must obtain separate and explicit consent from the data subject.

Question #18 Which of the following statements about consent requirements for personal sensitive information under GB/T 35273-2020 is CORRECT?

A. Only explicit consent is required and separate consent is not needed

B. Both separate consent and explicit consent are mandatory

C. Bundled consent with other authorization items is allowed

D. Implied consent through continued use is lawful

Answer: B

Explanation: GB/T 35273-2020 stipulates that processing personal sensitive information requires both separate consent (not bundled with other matters) and explicit consent (clear, voluntary, specific expression of intention) before the Personal Information Protection Law was implemented.

Question #19 According to the Personal Information Protection Law and relevant app compliance regulations in China, may an app set the consent to its privacy policy as pre-checked by default?

A. Yes, it is allowed for user convenience

B. No, pre-checked default consent is strictly prohibited

C. Yes, if the privacy policy is posted publicly

D. Yes, if users can uncheck the option manually

Answer: B

Explanation: Chinese laws and app regulatory rules clearly ban pre-checked default consent for privacy policies; consent must be provided actively and explicitly by users without pre-selection.

Question #20 Which of the following behaviors complies with China’s requirements for app privacy policy consent?

A. Set the consent to privacy policy as pre-checked by default

B. Obtain active and explicit consent from users without pre-selection

C. Bundle privacy policy consent with other service authorizations

D. Use vague notice and default consent for privacy policy

Answer: B

Explanation: Legally compliant consent requires users to voluntarily and explicitly confirm agreement to the app’s privacy policy; default pre-check, bundled consent and vague notice are all illegal.

Question #21 According to Article 26 of the Personal Information Protection Law of the People's Republic of China, which of the following is a required measure for installing cameras in public places **for public security purposes**?

A. Install cameras without any conspicuous prompts

B. Set up prominent notification signs to inform the public

C. Use collected facial information for commercial marketing freely

D. Install cameras beyond the scope necessary for public security

Answer: B

Explanation: For installing image collection equipment in public places for public security purposes, a conspicuous prompt must be set up, and the collected information can only be used for

public security; installation without prompts, excessive collection and commercial use are prohibited.

Question #22 According to Article 26 of the Personal Information Protection Law of the People's Republic of China, which of the following is a mandatory measure for installing cameras in public places for non-public security purposes?

A. Collect personal images without obtaining individual consent

B. Use the data only for public security and no other purposes

C. Obtain separate consent from individuals before using relevant data

D. Install hidden cameras without any notification

Answer: C

Explanation: When installing cameras in public places for non-public security purposes, the processor must obtain separate consent from individuals; unauthorized collection, hidden installation and non-compliance use are in violation of the law.

Question #23 According to the Civil Code, the Consumer Rights Protection Law and the Law on the Protection of Minors of the People's Republic of China, which of the following statements is CORRECT?

A. Natural persons’ personal information is not protected by the Civil Code

B. Consumer associations are the main institutions protecting consumer rights under the Consumer Rights Protection Law

C. Online game service providers may offer services to minors from 22:00 to 08:00 the next day

D. The Consumer Rights Protection Law does not specify any institutions for consumer rights protection

Answer: B

Explanation: The Civil Code clearly protects the personal information of natural persons; consumer associations are the main social institutions protecting consumer rights as stipulated in the Consumer Rights Protection Law; online game providers are prohibited from providing services to minors during 22:00–08:00 next day per the Law on the Protection of Minors.

Question #24 Employee A was caught stealing during non-working hours, and the company dismissed A and issued a disciplinary notice disclosing A’s full name and department. Under the Personal Information Protection Law of China, which statement is CORRECT?

A. The company’s measure is lawful because A violated the law

B. The company’s measure is improper as it excessively processes personal information without legal basis

C. The company may publicly disclose employees’ personal information for internal discipline

D. The company has the right to publish any information related to employee violations

Answer: B

Explanation: Under the Personal Information Protection Law, an employer’s processing of employee personal information shall follow the principles of legality, legitimacy and necessity. Publicly disclosing an employee’s name and department for a non-working-hour illegal act lacks legal basis and constitutes excessive processing of personal information, which violates the law.

Question #25 According to Article 4 of the Measures for the Security Assessment of Cross-Border Data Transfers, which cumulative data scale triggers a mandatory cross-border data security assessment when providing data overseas since January 1 of the previous year?

A. 50,000 personal information items or 5,000 sensitive personal information items

B. 100,000 personal information items or 10,000 sensitive personal information items

C. 200,000 personal information items or 20,000 sensitive personal information items

D. 500,000 personal information items or 50,000 sensitive personal information items

Answer: B

Explanation: Pursuant to Article 4 of the Measures for the Security Assessment of Cross-Border Data Transfers, a data processor shall declare a cross-border data security assessment if it has cumulatively provided personal information of 100,000 individuals or sensitive personal information of 10,000 individuals to overseas recipients since January 1 of the previous year.

Question #26 According to Article 4 of the Measures for the Security Assessment of Cross-Border Data Transfers, which of the following entities must declare a cross-border data security assessment when providing personal information overseas?

A. A data processor processing personal information of 500,000 individuals

B. A critical information infrastructure operator (CIIO)

C. A data processor that has never provided data overseas

D. A data processor processing only non-personal business data

Answer: B

Explanation: Pursuant to Article 4 of the Measures for the Security Assessment of Cross-Border Data Transfers, critical information infrastructure operators and data processors processing personal information of more than 1 million individuals shall declare a cross-border data security assessment when providing personal information to overseas recipients.

Question #27 According to Article 55 of the Personal Information Protection Law of the People's Republic of China, which of the following personal information processing activities requires a prior personal information protection impact assessment?

A. Internal use of non-sensitive personal information for daily internal management

B. Processing sensitive personal information

C. Collecting public information that does not identify natural persons

D. Storing non-personal business data internally

Answer: B

Explanation: According to Article 55 of the Personal Information Protection Law, processing sensitive personal information is a

statutory scenario that requires a prior personal information protection impact assessment.

Question #28 According to Article 55 of the Personal Information Protection Law of the People's Republic of China, which of the following activities does NOT require a prior personal information protection impact assessment?

A. Using personal information to conduct automated decision-making

B. Providing personal information to overseas recipients

C. Collecting ordinary non-sensitive personal information for basic business services

D. Disclosing personal information to the public

Answer: C

Explanation: According to Article 55 of the Personal Information Protection Law, mandatory assessment scenarios include processing sensitive personal information, automated decision-making, entrusting/providing/disclosing personal information, cross-border data provision, etc. Collecting ordinary non-sensitive personal information for basic services is not included.

Question #29 According to Articles 36 and 40 of the Personal Information Protection Law, which of the following is required when a state organ really needs to provide the personal information it processes to overseas recipients?

A. No security assessment is required, only filing with the local competent authority is needed

B. Conduct a security assessment in accordance with relevant provisions

C. Only obtain the explicit consent of the data subject

D. Entrust a third-party institution to conduct a risk assessment instead

Answer: B

Explanation: Pursuant to Article 36 of the Personal Information Protection Law, state organs shall store the personal information they process within the territory of the People's Republic of China; if it is really necessary to provide it overseas, a security assessment shall be conducted.

Question #30 According to Articles 36 and 40 of the Personal Information Protection Law, which of the following statements about critical information infrastructure operators (CIIOs) providing personal information overseas is CORRECT?

A. CIIOs may directly provide personal information collected in China to overseas recipients

B. If CIIOs really need to provide personal information overseas, they shall pass the security assessment organized by the national cyberspace administration

C. CIIOs only need to conduct an internal security assessment without reporting to the competent authority

D. CIIOs may skip the security assessment if they have obtained the written consent of all data subjects

Answer: B

Explanation: Pursuant to Article 40 of the Personal Information Protection Law, CIIOs shall store the personal information collected and generated in China within the territory; if it is really necessary to provide it overseas, they shall pass the security assessment organized by the national cyberspace administration, unless otherwise stipulated by laws, administrative regulations and the national cyberspace administration.

Question #31 According to the Judicial Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving the Infringement of Citizens'

Personal Information, how many pieces of specially sensitive personal information (such as location tracking information and communication content) need to be illegally obtained, sold or provided to constitute a crime?

A. 50 pieces or more

B. 500 pieces or more

C. 5,000 pieces or more

D. 10,000 pieces or more

Answer: A

Explanation: The Judicial Interpretation clearly classifies personal information into three tiers based on sensitivity and sets corresponding conviction standards. For specially sensitive personal information including location tracking information, communication content, credit information and property information, illegally obtaining, selling or providing 50 pieces or more shall be deemed "serious circumstances" and constitute the crime of infringing on citizens' personal information.

Question #32 According to the Judicial Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving the Infringement of Citizens'

Personal Information, which of the following statements about the conviction standard for ordinary personal information is CORRECT?

A. Illegally obtaining 500 pieces of ordinary personal information constitutes a crime

B. Illegally selling 5,000 pieces of ordinary personal information constitutes a crime

C. Illegally providing 1,000 pieces of ordinary personal information constitutes a crime

D. Ordinary personal information is not subject to quantitative conviction standards

Answer: B

Explanation: Ordinary personal information refers to personal information other than specially sensitive and generally sensitive personal information (such as name, ID number and mobile phone number). Pursuant to the Judicial Interpretation, illegally obtaining, selling or providing 5,000 pieces or more of such information shall be identified as "serious circumstances" and constitute the crime of infringing on citizens' personal information. Options A and C are incorrect because their quantities do not meet the statutory conviction standards, and Option D is incorrect because ordinary

personal information has clear quantitative conviction requirements.

Question #33 In a Sino-foreign cooperative scientific research project, the cooperative parties need to transport human genetic resource materials collected in China overseas for research purposes. According to the Regulations on the Administration of Human Genetic Resources of China, which of the following practices is legally compliant?

A. Directly transport the materials overseas after obtaining the consent of both cooperative parties

B. Apply to the National Health Commission (NHC) for approval and obtain an exit certificate before transportation

C. Only complete the customs declaration procedures without going through any approval formalities

D. Transport the materials overseas after simple desensitization without approval

Answer: B

Explanation: Pursuant to Article 27 of the Regulations on the Administration of Human Genetic Resources, if it is really necessary to transport, mail or carry human genetic resource materials out of the country in Sino-foreign cooperative scientific

research projects, the applicant shall meet the statutory conditions, apply to the NHC for approval, and obtain an exit certificate for human genetic resource materials before going through customs procedures. Direct transportation, skipping approval or only completing customs declaration without approval are all illegal.

Question #34 According to the Regulations on the Administration of Human Genetic Resources and relevant laws of China, which of the following statements about the outbound provision of human genetic resource information in Sino-foreign cooperative projects is CORRECT?

A. Human genetic resource information can be provided to foreign cooperative parties without any filing procedures

B. If providing human genetic resource information overseas may affect national security, it shall pass the security review organized by the NHC

C. Foreign organizations can independently collect and provide human genetic resource information from China overseas

D. It is not necessary to conduct ethical review when providing human genetic resource information overseas

Answer: B

Explanation: Pursuant to Article 28 of the Regulations on the Administration of Human Genetic Resources, providing or opening the use of human genetic resource information to foreign organizations, individuals and their established or actually controlled institutions shall not endanger national security and public interests; if it may affect national security and public interests, it shall pass the security review organized by the NHC. In addition, it is required to file with the NHC and submit information backups. Foreign organizations are prohibited from independently collecting and providing China's human genetic resource information overseas, and ethical review is a necessary prerequisite for outbound provision, so other options are incorrect.

Question #35 According to the Personal Information Protection Law and the rules on employee personal information protection, which of the following acts by an employer complies with the principles of personal information protection?

A. Collect employees’ private life photos and family financial status that are unnecessary for work

B. Process employees’ personal information only for job management purposes and limit the scope to the minimum necessary

C. Disclose employees’ personal information to external partners for business promotion without consent

D. Retain employees’ personal information permanently even after resignation

Answer: B

Explanation: Employers processing employees' personal information shall abide by the principles of legality, legitimacy, necessity and good faith as well as data minimization. Processing only for work-related purposes and limiting to the minimum necessary scope is compliant; collecting unnecessary information, disclosing without consent and permanent retention violate personal information protection rules.