考试样卷

202301 版本

目录

考试说明

本试卷是 EXIN Privacy & Data Protection Professional (PDPP.CH)模拟考试。EXIN 考试准则适用于该考试。

本试卷由 40 道单项选择题组成。每道选择题有多个选项，但这些选项中只有一个是正确答案。

本试卷的总分是 40 分。每道题的分数是 1 分。您需要获得 26 分或以上通过考试。

考试时间为 120 分钟。

在该考试过程中您可以参考 GDPR。

祝您好运!

考试样卷

1 / 40

某公司实施一项隐私政策，以帮助证明其遵守GDPR。有许多将该政策公开的理由。

将隐私政策公开的**主要**原因是什么?

A company implements a privacy policy, which helps to demonstrate compliance with the GDPR. It is recommended that this policy is made publicly accessible for several reasons.

What is the **main** reason for making the privacy policy publicly available?

A) 为了让客户和合作伙伴确认组织必须处理哪些个人数据
To allow customers and partners to verify which personal data the organization must process

B) 为了让客户、合作伙伴和监管机构评估个人数据的处理方式
To allow customers, partners and the supervisory authority to assess how personal data are handled

C) 为了传达组织执行的数据保护影响评估（DPIAs）的结果
To communicate the result of data protection impact assessments (DPIAs) performed in the organization

D) 通知监管机构组织在发生个人数据泄露事故后将会如何应对
To inform the supervisory authority of how the organization will respond after personal data breaches

2 / 40

根据GDPR，哪项信息**不是**隐私政策的强制性部分?

According to the GDPR, what information is **not** a mandatory part of a privacy policy?

A) 有关个人数据跨境传输到第三国的信息
Information about international transfers of personal data to a third country

B) 有关控制者身份和联系方式的信息
Information about the identity and contact details of the controller

C) 有关组织中的数据安全措施的信息
Information relating to data security measures in the organization

D) 有关数据保留期和数据主体权利的信息
Information relating to retention periods and data subject's rights

3 / 40

GDPR采纳了"基于设计和默认的隐私"的有关原则。应用这些原则包括实施技术与组织措施。

为什么还需要实施组织措施?

The GDPR embraces the principles of privacy by design and by default. The application of these principles includes the implementation of both technical and organizational measures.

Why are organizational measures necessary?

A) 因为"基于设计和默认的隐私"要求组织将个人数据访问权仅限于控制者
Because privacy by design and by default requires that the organization restricts personal data access to controllers only

B) 因为保护数据主体的权利需要借助技术措施无法替代的组织流程
Because protecting the rights of data subjects, requires organizational processes that technical measures cannot cover

C) 因为任命数据保护官（DPO）（当在强制要求的情况下），被视为一种组织措施
Because the designation of a data protection officer (DPO), where mandatory, is regarded as an organizational measure

4 / 40

某公司正在启动一个项目来为消费者提供新的免费服务。

根据"隐私预设"的理念，何时是讨论数据保护的**最**理想时机?

A company is setting up a project to create a new, free service for consumers.

According to privacy by design, what is the **most** desirable moment to discuss data protection?

A) 从项目一开始
From the start of the project

B) 在实施阶段
During the implementation phase

C) 项目接近完成时
When the project nears completion

5 / 40

某组织正在使用ISO/IEC 27701标准来实施隐私信息管理系统（PIMS）。

在实施过程中，该组织的一些承包商意识到他们必须遵守不同国家的多项法律要求。这些承包商决定向数据保护官（DPO）征求意见。

根据ISO/IEC 27701，数据保护官应将法律要求归为什么类别?

An organization is implementing the privacy information management system (PIMS) using the ISO/IEC 27701 standard.

During the implementation, some of the organization's contractors realize that they must comply with several legal requirements from different countries. The contractors decide to ask the data protection officer (DPO) for advice.

According to ISO/IEC 27701, how should the DPO categorize the legal requirements?

A) 内部问题，因为法律要求会作为一项内部事宜直接影响PIMS。
Internal issue because the legal requirements directly impact the PIMS, which is an internal matter.

B) 内部问题，因为关联的要素是必须视为同事的承包商。
Internal issue because the relevant factors are the contractors who must be seen as coworkers.

C) 外部问题，因为承包商的工作有别于组织的正式员工。
External issue because the contractors operate outside the regular coworkers of the organization.

D) 外部问题，因为法律要求与组织有涉但独立于组织。
External issue because the legal requirements are relevant but independent from the organization.

6 / 40

某企业对消费者（B2C）组织正在实施隐私信息管理系统（PIMS）。

数据保护官（DPO）发现包含以下信息的媒介：

- 一个**外置硬盘**，其中包含竞争对手信息及其优劣势说明。
- 若干人力资源部（HR）的**纸质文件**，其中包含健康信息和紧急联系人信息。
- 一台计算机**服务器**，其中所有客户数据的备份，包括直接消费者的数据。
- 若干旧**U盘**，其中包含前同事的个人信息及其在组织的最后薪水。

哪个媒介**没有**必要成为PIMS的一部分？

A business to consumer (B2C) organization is implementing a privacy information management system (PIMS).

The data protection officer (DPO) comes across the following media that contain information:

- An **external hard drive** with competitor information and a description of their strengths and weaknesses.
- Some **paper files** from human resources (HR) with health information and emergency contact information in them.
- A computer **server** which contains a backup of all customer data, including of direct consumers.
- Old **USB drives** with former coworkers' personal information and their last salaries at the organization.

Which media do **not** have to be part of the PIMS?

A) 外置硬盘
External hard drive

B) 纸质文件
Paper files

C) 服务器
Server

D) U盘
USB drives

7 / 40

在定义隐私信息管理系统（PIMS）时，会创建不同的文档。其中一份文档是适用性声明（SoA）。

什么是适用性声明（SoA）？

When defining a privacy information management system (PIMS), different documents are created. One of these documents is the statement of applicability (SoA).

What is a statement of applicability (SoA)?

A) SoA衡量处理数据对个人造成高风险的可能性。
The SoA gauges how likely it is that processing data results in a high risk to individuals.

B) SoA记录员工和客户个人数据的处理位置和方式。
The SoA records where and how personal data of employees and customers is processed.

C) SoA规定必须应用哪些控制措施管理或最大限度降低PIMS中的风险。
The SoA states which controls must be applied to manage or minimize risk within the PIMS.

8 / 40

无论从短期还是长期来看，能够展示公司政策、操作规程和作业指导书如何制定是隐私信息管理系统（PIMS）的基本要求。这确保了各项行动可追溯到有关的管理决定和政策，并确保其结果是可复现的。

这是指PIMS的哪项要求?

It is fundamental to a privacy information management system (PIMS), both in the short and long term, to be able to demonstrate how corporate policies, operating procedures, and work instructions are formulated. This ensures that actions are traceable to management decisions and policies, and that the results are reproducible.

Which requirement of the PIMS is this referring to?

A) 审计
Audit

B) 存档
Documentation

C) 管理评审
Management review

D) 适用性声明（SoA）
Statement of applicability (SoA)

9 / 40

为什么最高管理层应该审查隐私信息管理系统（PIMS）的进展情况?

Why should top management review the progress of the privacy information management system (PIMS)?

A) 确保PIMS符合所有相关法律要求
To ensure that the PIMS conforms with all relevant legal requirements

B) 确保PIMS具有充分的隐私控制来降低风险
To ensure that the PIMS has enough privacy controls to mitigate risks

C) 确保定期审计PIMS并编制文件
To ensure that the PIMS is audited regularly and is producing documents

D) 确保PIMS有效并满足公司要求
To ensure that the PIMS is effective and meets corporate requirements

10 / 40

对隐私信息管理系统（PIMS）进行审计有多种原因。

根据ISO/IEC 27701，PIMS审计的**主要**目标是什么?

Auditing the privacy information management system (PIMS) can be done for multiple reasons.

According to ISO/IEC 27701, what is the **main** objective of PIMS audits?

A) 确认符合相关国家和国际标准的要求
To confirm that requirements of the relevant national and international standards are maintained

B) 确定具体的关注领域并解决单个工作流程的选择问题
To identify specific areas of concern and address the selection of individual work processes

C) 涵盖法律法规的相关变更及其解读的更新
To include updates of relevant changes to legislation and regulations, and their interpretation

D) 监控管理体系要求与工作实践之间的一致性
To monitor conformity between the management system requirements and working practices

11 / 40

某组织实施了一套隐私信息管理系统（PIMS）。其具体的要求必须基于当地规则和合同要求。

由此组织的法律团队下一步应该做什么?

An organization implements a privacy information management system (PIMS). The specific requirements must be based on local rules and contractual requirements.

What should be the next step for the organization's legal team?

A) 聘请当地法律顾问提供指导，并将ISO/IEC 27701作为合同标准应用于客户和供应商
Hire local legal advice and guidance, and apply the ISO/IEC 27701 as the contractual standard to clients and suppliers

B) 查找适用的国际最佳实践，并审查所有涉及个人数据处理的合同
Look up the applicable international best practices, and review all contracts which involve personal data processing

C) 梳理适用的法律和相关法律制裁，并审查所有涉及个人数据处理的合同
Map the applicable legislation and related legal sanctions, and review all contracts which involve personal data processing

D) 寻求当地监督机构的指导，并将ISO/IEC 27701作为合同标准应用于客户和供应商
Request local supervisory authority's guidance, and apply the ISO/IEC 27701 as a contractual standard to clients and suppliers

12 / 40

某组织正在与另一家公司合并。该组织已经实施了隐私信息管理系统（PIMS）。

这一过程是否完成取决于能否证明所有个人数据处理操作均遵循ISO/IEC 27701和适用的法律。

哪一项是**最**适当的证明方式?

An organization is merging with another company. The organization already has a privacy information management system (PIMS).

The completion of the process depends on demonstrating that all the personal data processing operations follow the ISO/IEC 27701 and the applicable legislation.

What is the **most** appropriate means to show this?

A) 数据保护影响评估（DPIA）报告
A data protection impact assessment (DPIA) report

B) 隐私影响评估（PIA）报告
A privacy impact assessment (PIA) report

C) 最近的PIMS审计报告
A recent PIMS audit report

D) 适用性声明（SoA）报告
A statement of applicability (SoA) report

13 / 40

某小型组织开发了一项成功的软件服务。他们的服务取得了巨大成功，这意味着组织需要更强健的云解决方案。因此，组织必须挑选一个外部云供应商。

该组织已通过ISO/IEC 27701认证。在寻找供应商时，组织发现了多家云供应商。一些供应商通过了ISO/IEC 27701认证，另一些未通过。

ISO/IEC 27701认证如何有助于进行供应商筛选?

A small organization has developed a successful software service. Their service is a large success, which means the organization needs a more robust cloud solution. Therefore, the organization must select an external cloud supplier.

The organization is ISO/IEC 27701 certified. When searching for a supplier, the organization comes across several cloud suppliers. Some suppliers are ISO/IEC 27701 certified, but others are not.

How can an ISO/IEC 27701 certification help with supplier selection?

A) 供应商的ISO/IEC 27701认证包括成本/效益分析，可确保降低服务成本。
The ISO/IEC 27701 certification of a supplier includes a cost/benefit analysis, which ensures lower costs for services.

B) 供应商的ISO/IEC 27701认证降低了供应商审计的必要性，给组织带来了便利。
The ISO/IEC 27701 certification of a supplier lowers the need for supplier audits, which is easier for the organization.

C) 组织的ISO/IEC 27701认证具有数据处理程序，可适用于任何供应商。
The ISO/IEC 27701 certification of the organization has procedures for data processing, which extends to any supplier.

D) 组织的ISO/IEC 27701认证要求供应商通过ISO/IEC 27701认证，这限制了选择范围。
The ISO/IEC 27701 certification of the organization requires an ISO/IEC 27701 certified supplier, which limits choices.

14 / 40

要获得ISO/IEC 27701认证将涉及几个管理系统。其中两个系统分别是：

-隐私信息管理系统（PIMS）
-信息安全管理系统（ISMS）

关于这两个系统的说法，哪一项是正确的?

When working towards ISO/IEC 27701 certification, there are several management systems involved. Two of these systems are:

- the privacy information management system (PIMS)
- the information security management system (ISMS)

What is true about these systems?

A) ISMS和PIMS审计可以合并进行，也可以单独进行，尽管PIMS的要求取决于ISMS的维护。
The ISMS and PIMS audits may be combined or done separately, even though the PIMS requirements depend on the maintenance of the ISMS.

B) ISMS和PIMS审计绝不能合并进行，因为PIMS和ISMS的系统要求互不依赖。
The ISMS and PIMS audits must never be done together, because the PIMS and ISMS system requirements do not depend on each other.

C) ISMS是PIMS的一部分并涉及信息保护，因为ISMS着眼于个人数据的业务风险方面。
The ISMS is part of the PIMS and addresses information protection, since the ISMS looks at a business risk approach to personal data.

15 / 40

某组织正在实施隐私信息管理系统（PIMS）。《通用数据保护条例》（GDPR）要求"个人数据的处理应确保个人数据的适当安全性和保密性[……]"。

此要求与ISO/IEC 27701标准之间有什么关系?

An organization is implementing a privacy information management system (PIMS). The GDPR requires that "personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data [...]".

What is the relationship between this requirement and the ISO/IEC 27701 standard?

A) GDPR的完整性和保密性原则构成了ISO/IEC 27701标准所要求的PIMS的基础。
The GDPR principles of integrity and confidentiality form the foundation of the PIMS that is required for the ISO/IEC 27701 standard.

B) GDPR的合法、公平和透明原则有助于PIMS和信息安全管理系统（ISMS）。
The GDPR principles of lawfulness, fairness, and transparency contribute to the PIMS and the information security management system (ISMS).

C) GDPR的目的限制原则明确规定了如何使用或不使用属于PIMS的数据。
The GDPR principle of purpose limitation prescribes exactly how the data that fall under the PIMS may or may not be used.

D) GDPR的存储限制原则说明了个人数据在处理前在PIMS中的保留时限。
The GDPR principle of storage limitation explains the length of time the personal data reside in the PIMS before processing.

16 / 40

ISO/IEC 27701标准中有一章专门介绍与ISO/IEC 27002标准相符的附加指南。

该章节**未**包含哪类建议?

The ISO/IEC 27701 standard contains a chapter dedicated to additional guidance that aligns with the ISO/IEC 27002 standard.

What type of recommendations are **not** included in this chapter?

A) 制定与信息安全方针相互独立或相结合的隐私政策
Develop privacy policies separate from or combined with information security policies

B) 确保至少对处理个人数据的所有员工进行意识培训
Ensure at least awareness training for all coworkers that handle or process personal data

C) 清晰标记所有数据，以识别个人数据存储或被处理的位置
Label all data clearly to identify where personal data is stored or otherwise processed

D) 根据审计范围规划以特定时间间隔计划内部和外部审计
Plan internal and external audits with a specific interval depending on the audit scope

17 / 40

应用隐私信息管理系统（PIMS）控制措施来管理风险并不容易，建议完成所有阶段的任务。

第一阶段是设计一套管理风险的控制措施。下面列出了其余阶段（随机排序）：

1. 对照控制措施与ISO/IEC 27701的附录A或附录B
2. 编制适用性声明（SoA）
3. 有效实施控制措施

其余阶段的**正确**顺序是什么?

Applying privacy information management system (PIMS) controls to manage risk is not an easy task, and it is recommended to go through all the stages.

The first stage is to design a set of controls to manage risks. The other stages are listed below (in random order):

1. Compare controls to ISO/IEC 27701's Annex A or B
2. Produce the statement of applicability (SoA)
3. Effectively implement the controls

What is the **correct** order of the other stages?

A) 1、2、3
1, 2, 3

B) 1、3、2
1, 3, 2

C) 2、1、3
2, 1, 3

D) 2、3、1
2, 3, 1

18 / 40

根据GDPR，哪一项活动始终由控制者负责?

According to the GDPR, which activity is always a responsibility of the controller?

A) 负责执行数据保护影响评估（DPIA）
Being responsible for performing a data protection impact assessment (DPIA)

B) 与安全公司签约以保护传输中的个人数据
Contracting a security company for the protection of personal data in transit

C) 采用新方法来收集客户的个人数据
Implementing a new method to collect personal data from the customers

D) 保存处理者执行的处理活动的记录
Maintaining records of the processing activities carried out by the processor

19 / 40

一家医院将其患者发票的打印工作外包给一家印刷公司。该印刷公司同时为其他组织打印发票。

因为一个纰漏，印刷公司在整理姓名和地址时弄混了，一些发票发错了患者。

这家医院之前已仔细分析过自己的流程，医院也已经建立了健全的验证程序，并与印刷公司签订了合同协议。

为什么这种情况下监管机构要追究医院的**责任**?

A hospital outsources its printing of patient invoices to a printing company. The printing company also prints invoices for other organizations.

Due to an error, names and addresses were mixed up when they were sorted at the printing company, and a number of invoices were sent to the wrong patients.

The hospital had carefully analyzed their own processes. The hospital had a robust verification process in place and has contractual agreements with the printing company.

Why will the hospital be held **responsible** by the supervisory authority?

A) 因为合同中明确了这一点
Because the contract determines this

B) 因为医院是控制者
Because the hospital is the controller

C) 因为混淆发生在患者之间
Because the mix-up is between patients

D) 因为验证出错
Because the verification has gone wrong

20 / 40

当控制者和处理者签订处理个人数据的合同时，二者同时承担特定的职责。其中一些职责由GDPR规定，其余可以在合同中约定。

根据GDPR，什么情况下处理者总是需要得到控制者的书面授权?

When a controller and a processor sign a contract for the processing of personal data, they both have specific responsibilities. Some of these responsibilities are prescribed by the GDPR and others can be arranged in the contract.

According to the GDPR, when does the processor always need written authorization by the controller?

A) 处理者与另一家公司签约，由该公司在数据传输期间来保护数据
When the processor contracts a company to protect data during transfers

B) 处理者与第三方签约，由该第三方处理个人数据
When the processor contracts a third party to process personal data

C) 处理者采用新方法收集个人数据
When the processor implements a new method to collect personal data

D) 处理者采用新方法删除个人数据
When the processor implements a new method to delete personal data

21 / 40

记录处理活动是谁的法律义务?

Who has the legal obligation to keep records of processing activities?

A) 首席信息官
The chief information officer

B) 首席隐私官
The chief privacy officer

C) 控制者和处理者
The controller and processor

D) 数据保护官（DPO）
The data protection officer (DPO)

22 / 40

设在欧洲经济区（EEA）的某北美组织正处理自然人的个人数据。他们处理的是大批量种族数据。

根据GDPR，在三种特定情况下，组织需要任命数据保护官（DPO）。

在本例中，出于什么原因该组织必须任命DPO?

A North American organization based in the EEA processes personal data of natural persons. It processes ethnicity data on a large scale.

According to the GDPR, an organization is required to appoint a data protection officer (DPO) in three specific cases.

In this case, for what reason is it mandatory for this organization to appoint a DPO?

A) 处理了外国人的个人数据
Foreigners' personal data are processed

B) 个人数据是由第三国处理
Personal data are processed by a third country

C) 处理了少数群体的个人数据
Personal data of minorities are processed

D) 处理了特殊类别的个人数据
Special categories of personal data are processed

23 / 40

某数据保护官（DPO）服务于一个国家的交通部。

该部门宣布了一个监控人们在国道上的驾驶行为的新项目。该交通部想用智能视频分析系统识别出每辆汽车并自动识别车牌。

国务卿急于启动该项目，且担心隐私问题可能会导致其不必要的延误。

该DPO应该怎么做?

A data protection officer (DPO) works for the Ministry of Transportation, which is a national department.

A new project is announced to monitor people's driving behavior on the national highways. The Ministry wants to use an intelligent video analysis system to single out cars and automatically recognize license plates.

The state secretary is in a hurry to get the project started and worries that privacy issues might cause unwelcome delays.

What should the DPO do?

A) 要求国务卿与监管机构联系，因为这显然超出了DPO的职责范围
Ask the state secretary to contact the supervisory authority, because this is clearly outside the DPO's scope

B) 如果数据主体被告知了该数据处理，则向国务卿保证不再需要数据保护影响评估（DPIA）不再需要
Assure the state secretary that a data protection impact assessment (DPIA) is unnecessary, if data subjects are informed of the data processing

C) 告知国务卿，公共场所的大规模监控必须执行DPIA
Inform the state secretary that a DPIA is mandatory for the large-scale monitoring of a public space

D) 敦促国务卿重新考虑该项目，因为大规模监控数据的处理是被禁止的
Urge the state secretary to reconsider the project, because mass surveillance data processing is prohibited

24 / 40

数据保护官（DPO）在执行其任务时受到保密要求的约束。

而涉及到哪一方时DPO可**免除**保密义务以寻求建议?

Data protection officers (DPOs) are bound by secrecy or confidentiality concerning the performance of their tasks.

In relation to which party is the DPO **exempted** from this secrecy or confidentiality to seek advice?

A) 公司董事会
The board of directors of the company

B) 数据和隐私保护成员小组
The data protection and privacy network members team

C) 信息安全官（ISO）
The information security officer (ISO)

D) 监管机构
The supervisory authority

25 / 40

数据保护影响评估（DPIA）是一种用于识别数据保护风险的手段，尤其是识别可能对自然人的权利和自由产生重大影响的风险。

为什么DPIA可以被视为更宽泛的组织风险管理工作中的一部分?

A data protection impact assessment (DPIA) is a tool to identify data protection risks, especially the ones which are likely to highly affect the rights and freedoms of natural persons.

Why can the DPIA be seen as part of an organization's wider risk management?

A) 因为DPIA会评估受审组织的所有安全风险，并取代任何其他风险评估或风险管理
Because the DPIA assesses all security risks of the organization under review and replaces any other risk assessment or risk management

B) 因为DPIA通过风险的可能性和严重性来评估风险，类似于风险管理明确定义的其他组成部分
Because the DPIA assesses risks by the likelihood and severity of the risk, similar to other well-defined components of risk management

C) 因为根据GDPR，每个项目都必须执行DPIA，从而减少风对险管理的其他法律要求
Because the DPIA is mandatory for each project, according to the GDPR, which reduces all other legal requirements for risk management

26 / 40

根据GDPR，什么应始终是数据保护影响评估（DPIA）中的一个环节?

According to the GDPR, what should always be part of a data protection impact assessment (DPIA)?

A) 制定一个数据主体查阅请求的程序，以确保遵从数据主体的权利
Develop a subject access request procedure to ensure compliance with data subjects' rights

B) 明确已处理的个人数据以及处理的预期目的
Identify the personal data that are processed and the intended purposes of the processing

C) 通知数据主体将进行评估并征得其明确同意
Notify the data subjects that an assessment will take place and request their explicit consent

D) 制定事故响应计划并定义适当的防护措施，以避免数据泄露
Set up an incident response plan and define appropriate safeguards to avoid data breaches

27 / 40

某组织开发一款新产品，用于发现表现不佳的员工。他们搜索员工的上网历史记录并使用人工智能（AI）分析其工作行为。

尽管软件工程师并不完全理解算法，但是管理层还是决定解雇表现垫底的10%员工。

数据保护官（DPO）对此产品的影响表示担忧，告知董事会需要执行一个数据保护影响评估（DPIA）。

什么**不是**此例必须执行DPIA的原因?

An organization develops a new product to find underperforming employees. They search their internet history and analyze work behavior using artificial intelligence (AI).

Although the software engineers do not fully understand the algorithm, management decides to fire the bottom 10% employees.

The data protection officer (DPO) is concerned about the impact of this product and informs the board that a data protection impact assessment (DPIA) is required.

What is **not** part of the reason why a DPIA is mandatory?

A) 个人数据处理的自动化
The automation of the personal data processing

B) 该评估可能显著影响数据主体
The evaluation that may affect the data subjects significantly

C) 处理特殊类别的个人数据
The processing of special categories of personal data

D) 系统评估自然人的个人方面
The systematic evaluation of personal aspects of natural persons

28 / 40

什么**不属于**数据保护影响评估（DPIA）的产出?

What is **not** an outcome of a data protection impact assessment (DPIA)?

A) 带有自动化授权检查的机密数据查阅日志
A log of access to confidential data, with an automated authorization check

B) 数据主体对预期处理工作的看法的记录
A record of data subjects' views on the intended processing operations

C) 对预期处理工作的系统描述
A systematic description of the intended processing operations

D) 评估对数据主体权利和自由造成的风险
An assessment of risks to the rights and freedoms of data subjects

29 / 40

GDPR详细说明了数据保护影响评估（DPIA）必须至少输出的内容。

什么**不属于**DPIA的强制要求的?

The GDPR details what the output of a data protection impact assessment (DPIA) must contain at a minimum.

What is **not** mandatory in a DPIA?

A) 描述处理工作及其目的
A description of the processing and its purposes

B) 评估处理工作相对于目的的必要性和相称性
An assessment of the necessity and proportionality of the processing operations in relation to the purposes

C) 评估对数据主体权利和自由造成的风险
An assessment of the risks to the rights and freedoms of data subjects

D) 监管机构的建议
The advice of the supervisory authority

30 / 40

一项数据保护影响评估（DPIA）表明，预期的处理工作将涉及到收集超出预期目的所必需的个体客户数据。

根据GDPR，什么是**最**恰当的应对?

A data protection impact assessment (DPIA) shows that the intended processing involves collecting more data on individual customers than is necessary to achieve the intended purpose.

According to the GDPR, what is the **most** appropriate response?

A) 尽快将数据匿名
Anonymize the data as soon as possible

B) 推出培训和意识培养计划
Introduce a training and awareness program

C) 限制数据存储的时长
Limit the period of time for which the data is stored

D) 减少数据收集量
Reduce the amount of data collected

31 / 40

在开始数据保护影响评估（DPIA）之前，最好**先**做什么?

What is best done **first**, before starting a data protection impact assessment (DPIA)?

A) 确定应对已识别风险的措施
Determining measures to address the identified risks

B) 确定是否需要执行DPIA
Determining whether there is a need for a DPIA

C) 识别对数据主体权利和自由造成的风险
Identifying the risks to the rights and freedoms of data subjects

32 / 40

某公司执行了一个数据保护影响评估（DPIA）。

为什么说绘制数据地图对其做DPIA有用?

A company performs a data protection impact assessment (DPIA).

Why is data mapping useful for a DPIA?

A) 它有助于评估所有隐私方面的组织风险。
It assesses all organizational risks to privacy.

B) 它有助于获得一个对使用中的个人数据的概览。
It helps to gain an overview of the personal data in use.

C) 它有助于告知所有相关方。
It helps to inform all relevant parties.

33 / 40

某组织聘请了一名隐私专家。该组织希望将部分数据处理活动外包。该专家对涉及一个数据处理者来做处理工作进行一项数据保护影响评估（DPIA）。

DPIA中一个主要的步骤中要求由控制者来给出所有意见，而不要求处理者参与。

该步骤具体指哪一步?

A privacy expert is hired by an organization. They wish to outsource part of their data processing activities. The expert performs a data protection impact assessment (DPIA) on the processing that involves a data processor.

One of the main steps of a DPIA requires the controller to provide all the input and does not require the processor to be involved.

Which step is that?

A) 评估处理的必要性和相称性
Assessment of the necessity and proportionality of the processing

B) 评估对数据主体权利和自由造成的风险
Assessment of the risks to the rights and freedoms of data subjects

C) 缓解风险的措施，包括保障措施
Mitigating measures to address the risks, including safeguards

D) 系统描述预期的处理工作
Systematic descriptions of the intended processing operations

34 / 40

一家大公司出现财务困难。董事会希望员工提高工作效率。

董事会决定开始一项试验，以监控员工的上网活动，并通过分析数据了解可以提高效率之处，而被归为*效率低下*的员工可能会被解雇。

为什么在采用该新程序之前必须进行一个数据保护影响评估（DPIA）？

A large company is struggling financially. The board wants employees to work more efficiently.

The board starts an experiment in which the internet activities of the employees are monitored. The data are analyzed to see where more efficiency can be achieved. People categorized as *inefficient* might be dismissed.

Why must a data protection impact assessment (DPIA) be done before using the new procedure?

A) 因为大公司会有大量员工。所以，处理工作将是大规模的。
Because a large company has many employees. Therefore, the processing will be large scale.

B) 因为这是一次试验。新的处理活动和试验性的处理活动都需要执行DPIA。
Because it is an experiment. A DPIA is required for new and experimental processing activities.

C) 因为这是一次系统性的处理，且相关决定可能会相当程度地影响员工。
Because it is systematic processing. The decisions might significantly affect the employees.

35 / 40

某组织计划基于特征分析对客户实行自动决策。

在此例中数据保护影响评估（DPIA）的哪一部分需要特别注意?

An organization plans to make automated decisions on its clients, based on profiling.

Which part of the data protection impact assessment (DPIA) needs extra attention?

A) 针对此处理活动执行DPIA的需求的评估
The assessment of the need to perform a DPIA in relation to this processing activity

B) 将要实施的保护数据主体权利的措施
The measures to protect the rights of the data subject that will be implemented

C) 保护个人数据免受数据主体请求的措施
The measures to secure the personal data from being requested by data subjects

D) 数据主体要求删除其数据后，用来数据擦除的程序
The procedures for data erasure after a data subject asks for their data to be removed

36 / 40

GDPR规定，组织必须设法防止个人数据泄露。因此，要快速识别可归类为个人数据泄露的事故。

根据GDPR，哪一项**不属于**个人数据泄露事故?

The GDPR states that organizations must seek ways to prevent personal data breaches. Therefore, it is important to quickly recognize incidents that can be classified as personal data breaches.

According to the GDPR, which incident is **not** a personal data breach?

A) 患者期望收到装有医疗设备的包裹，但是包裹却被送错地址。
A patient is expecting a package containing medical equipment, but it is delivered to the wrong address.

B) 在精神卫生诊所工作的一名雇员放错了一套患者档案而且无法追溯。
An employee working at a mental health clinic has misplaced a set of patient files that cannot be retraced.

C) 数据仓库因火灾或地震意外破坏了个人数据。
The accidental destruction of personal data by a fire or an earthquake in a data warehouse.

D) 未经授权披露了公司一个涉及计划收购的有关机密财务数据。
The unauthorized disclosure of a company's confidential financial data regarding an intended acquisition.

37 / 40

在什么情况下需要向监管机构上报个人数据泄露事故?

In which situation is it required to report a personal data breach to the supervisory authority?

A) 组织在事故发生后72小时内无法解决
If the organization cannot resolve the incident within a timeframe of 72 hours after it has occurred

B) 在对自然人的权利和自由构成安全威胁的任何情况下
In any situation where there is a security threat to the rights and freedom of natural persons

C) 只要在72小时内将事故确认为个人数据泄露事故
Only if the incident is recognized as a personal data breach within a timeframe of 72 hours

D) 个人数据泄露可能给自然人的权利和自由带来风险时
When a personal data breach is likely to result in a risk to the rights and freedom of natural persons

38 / 40

人力资源（HR）部主管丢失了一个存储卡，其中包含35名员工的个人信息。该存储卡有强加密的保护。人力资源部曾将这些个人信息存储在备份设备中。

根据GDPR，是否必须将这一个人数据泄露事故上报给监管机构?

The head of the Human Resources (HR) department has lost a memory stick containing the personal information of 35 employees. The memory stick is protected by strong encryption. The HR department also has this personal information stored in a backup device.

According to the GDPR, is it mandatory to report this personal data breach to the supervisory authority?

A) 是，因为所有安全事件都必须上报给监管机构。
Yes, because all security incidents must be reported to the supervisory authority.

B) 是，因为报告监管机构后可以让其通知员工。
Yes, because reporting it enables the supervisory authority to inform the employees.

C) 否，因为报告数据泄露不符合公司的合法利益。
No, because it is not a legitimate interest of the company to report data breaches.

D) 否，因为该个人数据泄露事故不会对数据主体的权利造成风险。
No, because this personal data breach creates no risk to the data subjects' rights.

39 / 40

根据GDPR，在什么情况下必须将个人数据泄露事故报告给受影响的数据主体?

According to the GDPR, in which situation must a personal data breach be reported to the data subjects affected?

A) 个人数据泄露可能给数据主体的权利和自由带来高风险时
When a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject

B) 监管机构判定同意是处理的唯一法律依据时
When the supervisory authority has determined that consent was the only legal ground for processing

C) 当一个安全事故在72小时内被列为个人数据泄露事故时
When there is a security incident that is labelled as a personal data breach within 72 hours

D) 个人数据受到黑客或其他网络罪犯等外部因素的破坏时
When personal data is compromised by external factors such as hackers or other cyber criminals

40 / 40

在事故响应的最佳实践中定义了准备、响应和跟进几个阶段。每个阶段都必须进行存档。

在响应阶段，重要的是收集和保存证据，证明事件发生的原因以及组织未能防止事故发生的原因。

其中具体必须收集和保存是哪一个?

In the best practice incident response process the phases prepare, respond and follow-up are defined. For each phase, documentation is essential.

In the respond phase, it is important to gather and preserve evidence to show why an incident happened and why the organization was not able to prevent the incident.

What must be gathered and preserved?

A) 审计控制计划
Audit control plans

B) 数据保护影响评估（DPIAs）
Data protection impact assessments (DPIAs)

C) 能提供清晰图景的证据
Evidence to provide a clear picture

D) 系统恢复计划
System recovery plans

答案解析

1 / 40

某公司实施一项隐私政策，以帮助证明其遵守GDPR。有许多将该政策公开的理由。

将隐私政策公开的**主要**原因是什么?

A company implements a privacy policy, which helps to demonstrate compliance with the GDPR. It is recommended that this policy is made publicly accessible for several reasons.

What is the **main** reason for making the privacy policy publicly available?

A) 为了让客户和合作伙伴确认组织必须处理哪些个人数据
To allow customers and partners to verify which personal data the organization must process

B) 为了让客户、合作伙伴和监管机构评估个人数据的处理方式
To allow customers, partners and the supervisory authority to assess how personal data are handled

C) 为了传达组织执行的数据保护影响评估（DPIAs）的结果
To communicate the result of data protection impact assessments (DPIAs) performed in the organization

D) 通知监管机构组织在发生个人数据泄露事故后将会如何应对
To inform the supervisory authority of how the organization will respond after personal data breaches

（题目未完，接下一页）

A) 错误。公开的隐私政策并不用来确立组织必须处理哪些个人数据，而是将个人数据处理透明化。
Incorrect. Publicly available privacy policies do not establish which personal data must be processed by the organization. They provide transparency to the personal data processing.

B) 正确。公开的政策保障透明度，允许客户和合作伙伴对其进行评估，明确表态监管机构和其他监管者可以据其评估组织。（文献：A，第16章）
Correct. A publicly available policy supports transparency, allows customers and partners to assess it, and provides a clear statement that supervisory authorities and other regulators can assess the organization against. (Literature: A, Chapter 16)

C) 错误。DPIAs的结果应记录在案，以供内部商讨，且不应包含在隐私政策中。
Incorrect. The result of the DPIAs are intended to be documented for internal consultation and should not be included in the privacy policy.

D) 错误。组织如何应对数据泄露事故是数据泄露应对计划的一部分，该计划属于内部文件，不需要公开。
Incorrect. How the organization responds to a data breach is part of the data breach response plan, which is an internal document and not required to be publicly available.

2 / 40

根据GDPR，哪项信息**不是**隐私政策的强制性部分?

According to the GDPR, what information is **not** a mandatory part of a privacy policy?

A) 有关个人数据跨境传输到第三国的信息
Information about international transfers of personal data to a third country

B) 有关控制者身份和联系方式的信息
Information about the identity and contact details of the controller

C) 有关组织中的数据安全措施的信息
Information relating to data security measures in the organization

D) 有关数据保留期和数据主体权利的信息
Information relating to retention periods and data subject's rights

A) 错误。这是强制性的。
Incorrect. This is mandatory.

B) 错误。这是强制性的。
Incorrect. This is mandatory.

C) 正确。这是信息安全政策的一部分。（文献：A，第16章；GDPR第13条）
Correct. This is part of an information security policy. (Literature: A, Chapter 16; GDPR Article 13)

D) 错误。这是强制性的。
Incorrect. This is mandatory.

3 / 40

GDPR采纳了"基于设计和默认的隐私"的有关原则。应用这些原则包括实施技术与组织措施。

为什么还需要实施组织措施?

The GDPR embraces the principles of privacy by design and by default. The application of these principles includes the implementation of both technical and organizational measures.

Why are organizational measures necessary?

A) 因为"基于设计和默认的隐私"要求组织将个人数据访问权仅限于控制者
Because privacy by design and by default requires that the organization restricts personal data access to controllers only

B) 因为保护数据主体的权利需要借助技术措施无法替代的组织流程
Because protecting the rights of data subjects, requires organizational processes that technical measures cannot cover

C) 因为任命数据保护官（DPO）（当在强制要求的情况下），被视为一种组织措施
Because the designation of a data protection officer (DPO), where mandatory, is regarded as an organizational measure

A) 错误。组织措施旨在保护数据主体的权利，包括公平、透明的处理程序。
Incorrect. Organizational measures are meant to protect the data subjects' rights and consist of procedures for fair and transparent processing.

B) 正确。某些内部流程和程序必须通过组织措施解决，以确保数据主体的权利可以完全遵照GDPR行使。技术工具和系统是对组织措施的补充，但不能作为替代。（文献：A，第9章）
Correct. Some internal processes and procedures must be addressed by organizational measures to guarantee that the data subjects rights can be fully exercised in compliance with the GDPR. Technical tools and systems complement the organizational measures, but do not substitute them. (Literature: A, Chapter 9)

C) 错误。组织措施旨在保护数据主体的权利，包括公平、透明的处理程序。
Incorrect. Organizational measures are meant to protect the data subjects' rights and consist of procedures for fair and transparent processing.

4 / 40

某公司正在启动一个项目来为消费者提供新的免费服务。

根据"隐私预设"的理念，何时是讨论数据保护的**最**理想时机?

A company is setting up a project to create a new, free service for consumers.

According to privacy by design, what is the **most** desirable moment to discuss data protection?

A) 从项目一开始
From the start of the project

B) 在实施阶段
During the implementation phase

C) 项目接近完成时
When the project nears completion

A) 正确。要遵守隐私预设的原则，必须从项目一开始就对隐私和数据保护进行倡导。（文献：A，第5章；F）
Correct. Privacy and data protection must be promoted from the start of the project in line with the privacy by design principle. (Literature: A, Chapter 5; F)

B) 错误。在实施阶段讨论数据保护为时已晚。
Incorrect. Discussing data protection in the implementation phase is too late.

C) 错误。在项目完成阶段讨论数据保护为时已晚。
Incorrect. Discussing data protection in the project completion phase is too late.

5 / 40

某组织正在使用ISO/IEC 27701标准来实施隐私信息管理系统（PIMS）。

在实施过程中，该组织的一些承包商意识到他们必须遵守不同国家的多项法律要求。这些承包商决定向数据保护官（DPO）征求意见。

根据ISO/IEC 27701，数据保护官应将法律要求归为什么类别?

An organization is implementing the privacy information management system (PIMS) using the ISO/IEC 27701 standard.

During the implementation, some of the organization's contractors realize that they must comply with several legal requirements from different countries. The contractors decide to ask the data protection officer (DPO) for advice.

According to ISO/IEC 27701, how should the DPO categorize the legal requirements?

A) 内部问题，因为法律要求会作为一项内部事宜直接影响PIMS。
Internal issue because the legal requirements directly impact the PIMS, which is an internal matter.

B) 内部问题，因为关联的要素是必须视为同事的承包商。
Internal issue because the relevant factors are the contractors who must be seen as coworkers.

C) 外部问题，因为承包商的工作有别于组织的正式员工。
External issue because the contractors operate outside the regular coworkers of the organization.

D) 外部问题，因为法律要求与组织有涉但独立于组织。
External issue because the legal requirements are relevant but independent from the organization.

（题目未完，接下一页）

A) 错误。尽管法律要求可能会直接影响PIMS，但法律要求本身始终是外部问题。
Incorrect. Although the legal requirements will likely directly impact the PIMS, the legal requirements themselves are always external issues.

B) 错误。虽然承包商确实必须被视为同事，而员工管理和报告是内部问题，但这里要被归类的要素是法律要求。
Incorrect. Although contractors must indeed be seen as coworkers and staff management and reporting are internal issues, the factors to be categorized are the legal requirements.

C) 错误。所有的同事，包括外部承包商的管理和报告都必须被视为内部问题。此外，这里要被归类的要素是法律要求，其属于外部问题。
Incorrect. All coworkers, including external contractors, their management and reporting must be considered internal issues. Additionally, the factors to be categorized are the legal requirements, which are external issues.

D) 正确。根据ISO/IEC 27701引入的条款，法律要求被视为外部问题。（文献：B，第2章）
Correct. According to the term introduced by ISO/IEC 27701, legal requirements are considered external issues. (Literature: B, Chapter 2)

6 / 40

某企业对消费者（B2C）组织正在实施隐私信息管理系统（PIMS）。

数据保护官（DPO）发现包含以下信息的媒介：

- 一个**外置硬盘**，其中包含竞争对手信息及其优劣势说明。
- 若干人力资源部（HR）的**纸质文件**，其中包含健康信息和紧急联系人信息。
- 一台计算机**服务器**，其中所有客户数据的备份，包括直接消费者的数据。
- 若干旧**U盘**，其中包含前同事的个人信息及其在组织的最后薪水。

哪个媒介**没有**必要成为PIMS的一部分？

A business to consumer (B2C) organization is implementing a privacy information management system (PIMS).

The data protection officer (DPO) comes across the following media that contain information:

- An **external hard drive** with competitor information and a description of their strengths and weaknesses.
- Some **paper files** from human resources (HR) with health information and emergency contact information in them.
- A computer **server** which contains a backup of all customer data, including of direct consumers.
- Old **USB drives** with former coworkers' personal information and their last salaries at the organization.

Which media do **not** have to be part of the PIMS?

A) 外置硬盘
External hard drive

B) 纸质文件
Paper files

C) 服务器
Server

D) U盘
USB drives

（题目未完，接下一页）

A) 正确。PIMS应关注个人信息，在本例中，外置硬盘不包含任何个人信息。（文献：B，第1章）
Correct. The PIMS should be concerned with personal information and in this case the external hard drive does not contain any personal information. (Literature: B, Chapter 1)

B) 错误。所有包含个人信息的媒介，甚至是非数字媒介，都应成为PIMS的一部分。人力资源部文件包含个人信息，所以必须纳入PIMS中。
Incorrect. All media, even non-digital media, that contain personal information should be part of the PIMS. The HR files contain personal information and must be in the PIMS.

C) 错误。所有包含个人信息的媒介，即使仅包含备份，都应成为PIMS的一部分。服务器包含消费者数据，属于自然人的数据，因此是个人信息。
Incorrect. All media, even if they only contain a backup, that contain personal information should be part of the PIMS. The server contains consumer data, which is data from natural persons and, therefore, personal information.

D) 错误。所有包含个人信息的媒介都应成为PIMS的一部分，即使这些信息是前同事的信息。
Incorrect. All media that contain personal information should be part of the PIMS, even if the information is of former coworkers.

7 / 40

在定义隐私信息管理系统（PIMS）时，会创建不同的文档。其中一份文档是适用性声明（SoA）。

什么是适用性声明（SoA）？

When defining a privacy information management system (PIMS), different documents are created. One of these documents is the statement of applicability (SoA).

What is a statement of applicability (SoA)?

A) SoA衡量处理数据对个人造成高风险的可能性。
The SoA gauges how likely it is that processing data results in a high risk to individuals.

B) SoA记录员工和客户个人数据的处理位置和方式。
The SoA records where and how personal data of employees and customers is processed.

C) SoA规定必须应用哪些控制措施管理或最大限度降低PIMS中的风险。
The SoA states which controls must be applied to manage or minimize risk within the PIMS.

A) 错误。这是数据保护影响评估（DPIA）的作用。
Incorrect. This is what the data protection impact assessment (DPIA) does.

B) 错误。这记录在处理活动记录（ROPA）中。
Incorrect. This is recorded in the recording of processing activities (ROPA).

C) 正确。根据ISO/IEC 27701，这是SoA的定义。（文献：B，第4章）
Correct. According to ISO/IEC 27701, this is the definition of an SoA. (Literature: B, Chapter 4)

8 / 40

无论从短期还是长期来看，能够展示公司政策、操作规程和作业指导书如何制定是隐私信息管理系统（PIMS）的基本要求。这确保了各项行动可追溯到有关的管理决定和政策，并确保其结果是可复现的。

这是指PIMS的哪项要求?

It is fundamental to a privacy information management system (PIMS), both in the short and long term, to be able to demonstrate how corporate policies, operating procedures, and work instructions are formulated. This ensures that actions are traceable to management decisions and policies, and that the results are reproducible.

Which requirement of the PIMS is this referring to?

A) 审计
Audit

B) 存档
Documentation

C) 管理评审
Management review

D) 适用性声明（SoA）
Statement of applicability (SoA)

（题目未完，接下一页）

A) 错误。一个管理体系的审计计划其主要目标是监控管理体系要求与工作实践之间的一致性。
Incorrect. A management system audit program has the main objective to monitor conformity between the management system requirements and working practices.

B) 正确。组织很可能会发现，保留可以调用的开发和活动记录以应未来之需是很有用的。许多项目会被记录下来，组织会根据需要长期保留数据。创建服务于审查和决策的业务活动记录也与此有关。（文献：B，第3章）
Correct. It is likely that the organization will find it useful to keep records of developments and activities upon which it can call should it need to in the future. Many of these items are recorded and the organization retains the data for as long as necessary. Creating records of operating activities for the purpose of review and decision making is also relevant. (Literature: B, Chapter 3)

C) 错误。管理评审是最高管理层审查PIMS从启动到实施的进展情况的程序。该程序确保PIMS的有力推进，并逐渐满足公司要求。
Incorrect. Management review is a procedure in which top management reviews the progress of the PIMS from its inception to operation. This procedure ensures that the PIMS' progress is effective and meets corporate requirements over time.

D) 错误。SoA是一份详细说明哪些控制措施适用于PIMS，哪些不适用的文件。
Incorrect. The SoA is a document that details which controls are applied within the PIMS and which are not.

9 / 40

为什么最高管理层应该审查隐私信息管理系统（PIMS）的进展情况?

Why should top management review the progress of the privacy information management system (PIMS)?

A) 确保PIMS符合所有相关法律要求
To ensure that the PIMS conforms with all relevant legal requirements

B) 确保PIMS具有充分的隐私控制来降低风险
To ensure that the PIMS has enough privacy controls to mitigate risks

C) 确保定期审计PIMS并编制文件
To ensure that the PIMS is audited regularly and is producing documents

D) 确保PIMS有效并满足公司要求
To ensure that the PIMS is effective and meets corporate requirements

A) 错误。这是PIMS内部的一项责任，不是管理评审的目的。
Incorrect. This is a responsibility within the PIMS, not the purpose of the management review.

B) 错误。这是PIMS内部的一项责任，不是管理评审的目的。
Incorrect. This is a responsibility within the PIMS, not the purpose of the management review.

C) 错误。这是PIMS内部的一项责任，不是管理评审的目的。
Incorrect. This is a responsibility within the PIMS, not the purpose of the management review.

D) 正确。最高管理层宜审查PIMS从启动到实施的进展情况，确保PIMS的有力推进，并逐渐满足公司要求。（文献：B，第3章）
Correct. It is appropriate that top management reviews the progress of the PIMS from its inception through to operation, ensuring that it is effective and meets corporate requirements over time. (Literature: B, Chapter 3)

10 / 40

对隐私信息管理系统（PIMS）进行审计有多种原因。

根据ISO/IEC 27701，PIMS审计的**主要**目标是什么?

Auditing the privacy information management system (PIMS) can be done for multiple reasons.

According to ISO/IEC 27701, what is the **main** objective of PIMS audits?

A) 确认符合相关国家和国际标准的要求
To confirm that requirements of the relevant national and international standards are maintained

B) 确定具体的关注领域并解决单个工作流程的选择问题
To identify specific areas of concern and address the selection of individual work processes

C) 涵盖法律法规的相关变更及其解读的更新
To include updates of relevant changes to legislation and regulations, and their interpretation

D) 监控管理体系要求与工作实践之间的一致性
To monitor conformity between the management system requirements and working practices

A) 错误。确认适用国际标准的要求是目标之一，但主要目标是监控管理体系要求与工作实践之间的一致性。
Incorrect. Confirming the requirements of the applicable international standards is part of the objectives, but the main objective is to monitor conformity between the management system requirements and working practices.

B) 错误。这是审计可提供的一部分改进内容，但并不是主要目标。
Incorrect. This is part of the improvements that audit can provide, but this is not a main objective.

C) 错误。这是审计可以提供的改进的一部分，但并不是主要目标。
Incorrect. This is part of the improvement opportunities that audit can provide, but this is not a main objective.

D) 正确。管理体系审计计划的主要目标是监控管理体系要求与工作实践之间的一致性。（文献：B，第3章）
Correct. The main objective of a management system audit program is to monitor conformity between the management system requirements and working practices. (Literature: B, Chapter 3)

11 / 40

某组织实施了一套隐私信息管理系统（PIMS）。其具体的要求必须基于当地规则和合同要求。

由此组织的法律团队下一步应该做什么?

An organization implements a privacy information management system (PIMS). The specific requirements must be based on local rules and contractual requirements.

What should be the next step for the organization's legal team?

A) 聘请当地法律顾问提供指导，并将ISO/IEC 27701作为合同标准应用于客户和供应商
Hire local legal advice and guidance, and apply the ISO/IEC 27701 as the contractual standard to clients and suppliers

B) 查找适用的国际最佳实践，并审查所有涉及个人数据处理的合同
Look up the applicable international best practices, and review all contracts which involve personal data processing

C) 梳理适用的法律和相关法律制裁，并审查所有涉及个人数据处理的合同
Map the applicable legislation and related legal sanctions, and review all contracts which involve personal data processing

D) 寻求当地监督机构的指导，并将ISO/IEC 27701作为合同标准应用于客户和供应商
Request local supervisory authority's guidance, and apply the ISO/IEC 27701 as a contractual standard to clients and suppliers

（题目未完，接下一页）

A) 错误。确定PIMS的具体要求需要考虑相应的当地规则和合同要求。如果法律团队已经熟悉当地立法，可能无需寻求当地法律顾问的意见，而且并非所有合同都必须将ISO/IEC 27701作为合同标准要求。
Incorrect. The specific requirements of a PIMS need to be determined considering the appropriate local rules and contractual requirements. There may be no need to request local legal advice if the legal team is already familiar with the local legislation, and not all contracts will necessarily have the ISO/IEC 27701 as contractual standard requirements.

B) 错误。确定PIMS的具体要求必须考虑合同要求和适用的当地立法，而不是国际最佳实践。
Incorrect. The specific requirements of a PIMS must be determined considering contractual requirements and the applicable local legislation, not international best practices.

C) 正确。确定PIMS的具体要求需要考虑相应的当地规则和合同要求。（文献：B，第4章）
Correct. The specific requirements of a PIMS need to be determined considering the appropriate local rules and contractual requirements. (Literature: B, Chapter 4)

D) 错误。确定PIMS的具体要求需要考虑相应的当地规则和合同要求。无需寻求当地监督机构的指导，而且并非所有合同都必须将ISO/IEC 27701作为合同标准要求。
Incorrect. The specific requirements of a PIMS need to be determined considering the appropriate local rules and contractual requirements. There is no need to request the local supervisory authority's guidance, and not all contracts will necessarily have the ISO/IEC 27701 as contractual standard requirements.

12 / 40

某组织正在与另一家公司合并。该组织已经实施了隐私信息管理系统（PIMS）。

这一过程是否完成取决于能否证明所有个人数据处理操作均遵循ISO/IEC 27701和适用的法律。

哪一项是**最**适当的证明方式?

An organization is merging with another company. The organization already has a privacy information management system (PIMS).

The completion of the process depends on demonstrating that all the personal data processing operations follow the ISO/IEC 27701 and the applicable legislation.

What is the **most** appropriate means to show this?

A) 数据保护影响评估（DPIA）报告
A data protection impact assessment (DPIA) report

B) 隐私影响评估（PIA）报告
A privacy impact assessment (PIA) report

C) 最近的PIMS审计报告
A recent PIMS audit report

D) 适用性声明（SoA）报告
A statement of applicability (SoA) report

（题目未完，接下一页）

A) 错误。DPIA报告通常记录了在项目实施前进行的风险评估。对于可能对个人产生高风险的处理，需要进行DPIA。
Incorrect. A DPIA report registers a risk assessment typically undertaken before the implementation of a project. A DPIA is required for processing that is likely to result in a high risk to individuals.

B) 错误。PIA报告记录了通常在项目实施前进行的风险评估。对于可能对个人造成高风险的处理，需要进行DPIA。
Incorrect. A PIA report registers a risk assessment typically undertaken before the implementation of a project. A DPIA is required for processing that is likely to result in a high risk to individuals.

C) 正确。审计报告找出实际实践与要求之间的一致性和不一致性。（文献：B，第3章）
Correct. Audit reports identify conformity and non-conformity between the actual practice and the requirements. (Literature: B, Chapter 3)

D) 错误。适用性声明（SoA）（声明而非报告）是一份详细说明哪些控制措施适用于PIMS，哪些不适用的文件，但不能保证其是否反映实际实践。此外，也不能保证是否合法。
Incorrect. The statement of applicability (SoA) (a statement, not a report) is a document that details which controls are applied within the PIMS and which are not, but there is no guarantee that it reflects the actual practice. It also does not guarantee legal compliance.

13 / 40

某小型组织开发了一项成功的软件服务。他们的服务取得了巨大成功，这意味着组织需要更强健的云解决方案。因此，组织必须挑选一个外部云供应商。

该组织已通过ISO/IEC 27701认证。在寻找供应商时，组织发现了多家云供应商。一些供应商通过了ISO/IEC 27701认证，另一些未通过。

ISO/IEC 27701认证如何有助于进行供应商筛选?

A small organization has developed a successful software service. Their service is a large success, which means the organization needs a more robust cloud solution. Therefore, the organization must select an external cloud supplier.

The organization is ISO/IEC 27701 certified. When searching for a supplier, the organization comes across several cloud suppliers. Some suppliers are ISO/IEC 27701 certified, but others are not.

How can an ISO/IEC 27701 certification help with supplier selection?

A) 供应商的ISO/IEC 27701认证包括成本/效益分析，可确保降低服务成本。
The ISO/IEC 27701 certification of a supplier includes a cost/benefit analysis, which ensures lower costs for services.

B) 供应商的ISO/IEC 27701认证降低了供应商审计的必要性，给组织带来了便利。
The ISO/IEC 27701 certification of a supplier lowers the need for supplier audits, which is easier for the organization.

C) 组织的ISO/IEC 27701认证具有数据处理程序，可适用于任何供应商。
The ISO/IEC 27701 certification of the organization has procedures for data processing, which extends to any supplier.

D) 组织的ISO/IEC 27701认证要求供应商通过ISO/IEC 27701认证，这限制了选择范围。
The ISO/IEC 27701 certification of the organization requires an ISO/IEC 27701 certified supplier, which limits choices.

（题目未完，接下一页）

A) 错误。ISO/IEC 27701认证不包括供应商列表。由于控制者始终负责确保数据保护，他们应对供应商进行审计。通过ISO/IEC 27701认证的供应商已经过审计。
Incorrect. An ISO/IEC 27701 certification does not include a list of suppliers. Since the controller is always responsible for ensuring data protection, they should audit suppliers. ISO/IEC 27701 certified suppliers already have been audited.

B) 正确。通过ISO/IEC 27701认证的供应商更有可能负责任地处理个人数据，并能够在个人数据泄露后更有效地合作。（文献：B，第5章）
Correct. An ISO/IEC 27701 certified supplier is more likely to process personal data responsibly and to be able to cooperate more effectively after a personal data breach. (Literature: B, Chapter 5)

C) 错误。控制者始终负责确保数据保护，所以他们应对供应商进行审计。通过ISO/IEC 27701认证的供应商已经过审计。
Incorrect. The controller will always remain responsible for ensuring data protection, which means they should audit suppliers. ISO/IEC 27701 certified suppliers already have been audited.

D) 错误。ISO/IEC 27701认证不要求所有供应商都通过相同的认证。由于控制者始终负责确保数据保护，所以他们应对供应商进行审计。通过ISO/IEC 27701认证的供应商已经过审计。
Incorrect. An ISO/IEC 27701 certification does not require all suppliers to have the same certification. Because the controller will always remain responsible for ensuring data protection, they should audit suppliers. ISO/IEC 27701 certified suppliers already have been audited.

14 / 40

要获得ISO/IEC 27701认证将涉及几个管理系统。其中两个系统分别是：

-隐私信息管理系统（PIMS）
-信息安全管理系统（ISMS）

关于这两个系统的说法，哪一项是正确的?

When working towards ISO/IEC 27701 certification, there are several management systems involved. Two of these systems are:

- the privacy information management system (PIMS)
- the information security management system (ISMS)

What is true about these systems?

A) ISMS和PIMS审计可以合并进行，也可以单独进行，尽管PIMS的要求取决于ISMS的维护。
The ISMS and PIMS audits may be combined or done separately, even though the PIMS requirements depend on the maintenance of the ISMS.

B) ISMS和PIMS审计绝不能合并进行，因为PIMS和ISMS的系统要求互不依赖。
The ISMS and PIMS audits must never be done together, because the PIMS and ISMS system requirements do not depend on each other.

C) ISMS是PIMS的一部分并涉及信息保护，因为ISMS着眼于个人数据的业务风险方面。
The ISMS is part of the PIMS and addresses information protection, since the ISMS looks at a business risk approach to personal data.

（题目未完，接下一页）

A) 正确。这两项审计可以合并进行。ISO/IEC 27701认证部分取决于ISO/IEC 27001认证和审计。（文献：B，第6章）
Correct. The two audits may be combined. ISO/IEC 27701 certification depends in part on ISO/IEC 27001 certifications and audits. (Literature B, Chapter 6)

B) 错误。这两项审计可以合并进行，也可以单独进行。ISO/IEC 27701认证部分取决于ISO/IEC 27001认证和审计。
Incorrect. The two audits may be combined or done separately. ISO/IEC 27701 certification depends in part on ISO/IEC 27001 certifications and audits.

C) 错误。ISMS旨在了解组织中所有数据的总体风险，并通过ISMS中的控制措施减轻这些风险。ISMS并不特别关注个人数据。
Incorrect. The ISMS is meant to get an idea of the risks to all data in general in the organization and mitigate those risks through the controls in the ISMS. The ISMS does not specifically focus on personal data.

15 / 40

某组织正在实施隐私信息管理系统（PIMS）。《通用数据保护条例》（GDPR）要求"个人数据的处理应确保个人数据的适当安全性和保密性[……]"。

此要求与ISO/IEC 27701标准之间有什么关系?

An organization is implementing a privacy information management system (PIMS). The GDPR requires that "personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data [...]".

What is the relationship between this requirement and the ISO/IEC 27701 standard?

A) GDPR的完整性和保密性原则构成了ISO/IEC 27701标准所要求的PIMS的基础。
The GDPR principles of integrity and confidentiality form the foundation of the PIMS that is required for the ISO/IEC 27701 standard.

B) GDPR的合法、公平和透明原则有助于PIMS和信息安全管理系统（ISMS）。
The GDPR principles of lawfulness, fairness, and transparency contribute to the PIMS and the information security management system (ISMS).

C) GDPR的目的限制原则明确规定了如何使用或不使用属于PIMS的数据。
The GDPR principle of purpose limitation prescribes exactly how the data that fall under the PIMS may or may not be used.

D) GDPR的存储限制原则说明了个人数据在处理前在PIMS中的保留时限。
The GDPR principle of storage limitation explains the length of time the personal data reside in the PIMS before processing.

（题目未完，接下一页）

A) 正确。数据安全性原则是PIMS的基本条件，确定适当个人数据安全性的GDPR原则称为"完整性和保密性"。因此，这一原则是PIMS的基础。（文献：B，第3章和GDPR，第5.1条第f款）
Correct. The data security principle is an essential condition for a PIMS and the GDPR principles that determine what is appropriate security of personal data is called 'integrity and confidentiality'. Therefore, these principles are the foundation of the PIMS. (Literature: B, Chapter 3 and GDPR, Art. 5.1.f)

B) 错误。PIMS可能有助于"合法、公平和透明"，但"完整性和保密性"原则是PIMS的基础。因此，后者与PIMS的关系最大。
Incorrect. The PIMS may contribute to the 'lawfulness, fairness and transparency', but the 'integrity and confidentiality' principle is the foundation for the PIMS. Therefore, the latter is the one which best relates to the PIMS.

C) 错误。PIMS可能有助于"目的限制"，但"完整性和保密性"原则是PIMS的基础。因此，后者与PIMS的关系最大。
Incorrect. The PIMS may contribute to the 'purpose limitation', but the 'integrity and confidentiality' principle is the foundation for the PIMS. Therefore, the latter is the one which best relates to the PIMS.

D) 错误。PIMS可能有助于"存储限制"，但"完整性和保密性"原则是PIMS的基础。因此，后者与PIMS的关系最大。
Incorrect. The PIMS may contribute to the 'storage limitation', but the 'integrity and confidentiality' principle is the foundation for the PIMS. Therefore, the latter is the one which best relates to the PIMS.

16 / 40

ISO/IEC 27701标准中有一章专门介绍与ISO/IEC 27002标准相符的附加指南。

该章节**未**包含哪类建议?

The ISO/IEC 27701 standard contains a chapter dedicated to additional guidance that aligns with the ISO/IEC 27002 standard.

What type of recommendations are **not** included in this chapter?

A) 制定与信息安全方针相互独立或相结合的隐私政策
Develop privacy policies separate from or combined with information security policies

B) 确保至少对处理个人数据的所有员工进行意识培训
Ensure at least awareness training for all coworkers that handle or process personal data

C) 清晰标记所有数据，以识别个人数据存储或被处理的位置
Label all data clearly to identify where personal data is stored or otherwise processed

D) 根据审计范围规划以特定时间间隔计划内部和外部审计
Plan internal and external audits with a specific interval depending on the audit scope

A) 错误。制定隐私政策的建议是该章节的一部分。
Incorrect. The recommendation on developing privacy policies is a part of this chapter.

B) 错误。该章节包含了至少进行一些培训的建议。
Incorrect. The recommendation of ensuring at least some training is in this chapter.

C) 错误。清晰标记所有数据的建议是该章节的一部分。
Incorrect. The recommendation to label all data clearly is part of this chapter.

D) 正确。尽管ISO/IEC 27701标准并未专门涉及合规性和审计，但该标准的制定与ISO/IEC 27001和ISO/IEC 27002相一致，其中包含这类类目。（文献：B，第5章）
Correct. Although the ISO/IEC 27701 standard does not specifically deal with compliance and audits, the standard is developed to align with ISO/IEC 27001 and ISO/IEC 27002, which do contain these categories. (Literature B, Chapter 5)

17 / 40

应用隐私信息管理系统（PIMS）控制措施来管理风险并不容易，建议完成所有阶段的任务。

第一阶段是设计一套管理风险的控制措施。下面列出了其余阶段（随机排序）：

1. 对照控制措施与ISO/IEC 27701的附录A或附录B
2. 编制适用性声明（SoA）
3. 有效实施控制措施

其余阶段的**正确**顺序是什么?

Applying privacy information management system (PIMS) controls to manage risk is not an easy task, and it is recommended to go through all the stages.

The first stage is to design a set of controls to manage risks. The other stages are listed below (in random order):

1. Compare controls to ISO/IEC 27701's Annex A or B
2. Produce the statement of applicability (SoA)
3. Effectively implement the controls

What is the **correct** order of the other stages?

A) 1、2、3
1, 2, 3

B) 1、3、2
1, 3, 2

C) 2、1、3
2, 1, 3

D) 2、3、1
2, 3, 1

（题目未完，接下一页）

A) 错误。正确的顺序是1、3、2。
Incorrect. The correct order is 1, 3, 2.

B) 正确。设计一套控制措施后，必须与ISO/IEC 27701的附录进行对照，以确保隐私风险保障达到要求的级别。然后应实施控制措施，最后是编制SoA。（文献：B，第4章）
Correct. After a set of controls is designed, the controls must be compared to ISO/IEC 27701's Annexes to ensure the required level of assurance against privacy risks. Then the controls should be implemented and the SoA follows last. (Literature: B, Chapter 4)

C) 错误。正确的顺序是1、3、2。
Incorrect. The correct order is 1, 3, 2.

D) 错误。正确的顺序是1、3、2。
Incorrect. The correct order is 1, 3, 2.

18 / 40

根据GDPR，哪一项活动始终由控制者负责?

According to the GDPR, which activity is always a responsibility of the controller?

A) 负责执行数据保护影响评估（DPIA）
Being responsible for performing a data protection impact assessment (DPIA)

B) 与安全公司签约以保护传输中的个人数据
Contracting a security company for the protection of personal data in transit

C) 采用新方法来收集客户的个人数据
Implementing a new method to collect personal data from the customers

D) 保存处理者执行的处理活动的记录
Maintaining records of the processing activities carried out by the processor

A) 正确。DPIA由控制者负责，不应外包给数据处理者。（文献：A，第12章；GDPR第35条）
Correct. Responsibility for DPIAs falls to the controller and should not be outsourced to a data processor. (Literature: A, Chapter 12; GDPR Article 35)

B) 错误。如果有事先书面授权，则由处理者负责。
Incorrect. This could be the responsibility of the processor, if prior written authorization exists.

C) 错误。如果有事先书面授权，则由处理者负责。
Incorrect. This could be the responsibility of the processor, if prior written authorization exists.

D) 错误。这是处理者负责的要素。控制者保存的是其控制下的处理活动的记录。
Incorrect. This element is the responsibility of the processor. The controller maintains a record of the processing activities they control.

19 / 40

一家医院将其患者发票的打印工作外包给一家印刷公司。该印刷公司同时为其他组织打印发票。

因为一个纰漏，印刷公司在整理姓名和地址时弄混了，一些发票发错了患者。

这家医院之前已仔细分析过自己的流程，医院也已经建立了健全的验证程序，并与印刷公司签订了合同协议。

为什么这种情况下监管机构要追究医院的**责任**?

A hospital outsources its printing of patient invoices to a printing company. The printing company also prints invoices for other organizations.

Due to an error, names and addresses were mixed up when they were sorted at the printing company, and a number of invoices were sent to the wrong patients.

The hospital had carefully analyzed their own processes. The hospital had a robust verification process in place and has contractual agreements with the printing company.

Why will the hospital be held **responsible** by the supervisory authority?

A) 因为合同中明确了这一点
Because the contract determines this

B) 因为医院是控制者
Because the hospital is the controller

C) 因为混淆发生在患者之间
Because the mix-up is between patients

D) 因为验证出错
Because the verification has gone wrong

（题目未完，接下一页）

A) 错误。医院被问责，是因为它作为控制者受制于GDPR规定的问责原则
Incorrect. The hospital is accountable because, as the controller, it is subject to the accountability principle, determined by the GDPR.

B) 正确。GDPR规定，“控制者应负责（见第1段：‘责任’）”处理的合法性。不论控制者与处理者签订何种合同，监管机构都要追究控制者责任。控制者应当仅使用能够充分保证实施适当技术和组织措施的处理者。（文献：A，第12章；GDPR，第5(2)条）
Correct. The GDPR states that “The controller shall be responsible [...], paragraph 1(‘accountability’)” for the lawfulness of processing. The controller will be held responsible and accountable by the supervisory authority, whatever contract may be in place between controller and processor. The controller should only use processors that provide sufficient guarantees that they implement appropriate technical and organizational measures. (Literature: A, Chapter 12; GDPR, article 5 (2))

C) 错误。数据主体都属于同一个控制者并不重要。本例中谁是控制者才重要。
Incorrect. It does not matter that the data subjects all belong to the same controller. Who is the controller is relevant here.

D) 错误。没有证据表明验证出错。监管机构将始终追究控制者责任。
Incorrect. There is nothing to indicate the verification went wrong. The supervisory authority will always hold the controller responsible.

20 / 40

当控制者和处理者签订处理个人数据的合同时，二者同时承担特定的职责。其中一些职责由GDPR规定，其余可以在合同中约定。

根据GDPR，什么情况下处理者总是需要得到控制者的书面授权?

When a controller and a processor sign a contract for the processing of personal data, they both have specific responsibilities. Some of these responsibilities are prescribed by the GDPR and others can be arranged in the contract.

According to the GDPR, when does the processor always need written authorization by the controller?

A) 处理者与另一家公司签约，由该公司在数据传输期间来保护数据
When the processor contracts a company to protect data during transfers

B) 处理者与第三方签约，由该第三方处理个人数据
When the processor contracts a third party to process personal data

C) 处理者采用新方法收集个人数据
When the processor implements a new method to collect personal data

D) 处理者采用新方法删除个人数据
When the processor implements a new method to delete personal data

A) 错误。该情况可能是处理者根据合同所决定的，因为GDPR并未明确定义。
Incorrect. This element is or might be at the determination of the processor according to the contract, as it is not clearly defined by the GDPR.

B) 正确。如果未取得控制者的事先具体或通用的书面授权，则不得聘请其他处理者。（文献：A，第12章；GDPR第28(2)条）
Correct. This engaging of another processor cannot be done without the prior specific or general written authorization of the controller. (Literature: A, Chapter 12; GDPR Article 28(2))

C) 错误。该情况可能是处理者根据合同所决定的，因为GDPR并未明确定义。
Incorrect. This element is or might be at the determination of the processor according to the contract, as it is not clearly defined by the GDPR.

D) 错误。该情况可能是处理者根据合同所决定的，因为GDPR并未明确定义。
Incorrect. This element is or might be at the determination of the processor according to the contract, as it is not clearly defined by the GDPR.

21 / 40

记录处理活动是谁的法律义务?

Who has the legal obligation to keep records of processing activities?

A) 首席信息官
The chief information officer

B) 首席隐私官
The chief privacy officer

C) 控制者和处理者
The controller and processor

D) 数据保护官（DPO）
The data protection officer (DPO)

A) 错误。首席信息官全权负责信息技术和信息管理。
Incorrect. The chief information officer has the overall responsibility for information technology and information management.

B) 错误。首席隐私官应让组织内部都参与到GDPR合规上来。
Incorrect. The chief privacy officer should create engagement for GDPR compliance within the organization.

C) 正确。控制者和处理者都需要保存所有处理活动的记录。（文献：A，第12章；GDPR第30条）
Correct. Both controller and processor are required to keep a record of all processing activities. (Literature: A, Chapter 12; GDPR Article 30)

D) 错误。尽管在实践中可能会由DPO创建清单、登记处理活动并承担保存这些记录的责任，但这都是基于在控制者或处理者的法律义务下来完成的。
Incorrect. Although in practice it is the DPO that creates inventories, holds a register of processing activities and has been given the responsibility to maintain these records, this is done under the legal obligation of the controller or processor.

22 / 40

设在欧洲经济区（EEA）的某北美组织正处理自然人的个人数据。他们处理的是大批量种族数据。

根据GDPR，在三种特定情况下，组织需要任命数据保护官（DPO）。

在本例中，出于什么原因该组织必须任命DPO?

A North American organization based in the EEA processes personal data of natural persons. It processes ethnicity data on a large scale.

According to the GDPR, an organization is required to appoint a data protection officer (DPO) in three specific cases.

In this case, for what reason is it mandatory for this organization to appoint a DPO?

A) 处理了外国人的个人数据
Foreigners' personal data are processed

B) 个人数据是由第三国处理
Personal data are processed by a third country

C) 处理了少数群体的个人数据
Personal data of minorities are processed

D) 处理了特殊类别的个人数据
Special categories of personal data are processed

（题目未完，接下一页）

A) 错误。这不是GDPR中规定的三个基本条件之一。
Incorrect. This is not one of the three basic conditions specified in the GDPR.

B) 错误。这不是GDPR中规定的三个基本条件之一。
Incorrect. This is not one of the three basic conditions specified in the GDPR.

C) 错误。这不是GDPR中规定的三个基本条件之一。
Incorrect. This is not one of the three basic conditions specified in the GDPR.

D) 正确。这是GDPR中规定的情况之一，其中控制者或处理者的核心活动包括第9条涉及的大批量处理特殊类别的数据。GDPR第9条特别提到了种族或人种数据。另外两个条件分别是：（1）处理工作是由公共机构或机关执行的，但以司法职能行事的法院除外；（2）处理工作需要对数据主体进行定期和系统的大规模监控。这三个基本条件同时适用于控制者和处理者。（文献：A，第2章；GDPR第9条和第37条）
Correct. This is one of the cases specified in the GDPR, when the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9. Ethnic or racial data is specifically mentioned in Article 9 of the GDPR. The other two conditions are: (1) processing is carried out by a public authority or body, except for courts acting in their judicial capacity, (2) processing that requires regular and systematic monitoring of data subjects on a large scale. These three basic conditions apply to both controllers and processors. (Literature: A, Chapter 2; GDPR Article 9 and Article 37)

23 / 40

某数据保护官（DPO）服务于一个国家的交通部。

该部门宣布了一个监控人们在国道上的驾驶行为的新项目。该交通部想用智能视频分析系统识别出每辆汽车并自动识别车牌。

国务卿急于启动该项目，且担心隐私问题可能会导致其不必要的延误。

该DPO应该怎么做?

A data protection officer (DPO) works for the Ministry of Transportation, which is a national department.

A new project is announced to monitor people's driving behavior on the national highways. The Ministry wants to use an intelligent video analysis system to single out cars and automatically recognize license plates.

The state secretary is in a hurry to get the project started and worries that privacy issues might cause unwelcome delays.

What should the DPO do?

A) 要求国务卿与监管机构联系，因为这显然超出了DPO的职责范围
Ask the state secretary to contact the supervisory authority, because this is clearly outside the DPO's scope

B) 如果数据主体被告知了该数据处理，则向国务卿保证不再需要数据保护影响评估（DPIA）不再需要
Assure the state secretary that a data protection impact assessment (DPIA) is unnecessary, if data subjects are informed of the data processing

C) 告知国务卿，公共场所的大规模监控必须执行DPIA
Inform the state secretary that a DPIA is mandatory for the large-scale monitoring of a public space

D) 敦促国务卿重新考虑该项目，因为大规模监控数据的处理是被禁止的
Urge the state secretary to reconsider the project, because mass surveillance data processing is prohibited

（题目未完，接下一页）

A) 错误。DPO应该有足够的资格对此进行讨论。
Incorrect. A DPO should be sufficiently qualified to discuss this.

B) 错误。告知数据主体不会免除组织执行DPIA的责任。
Incorrect. Informing data subjects will not exempt an organization from the responsibility to do a DPIA.

C) 正确。该项目需要对公共区域进行大规模的系统监控，这是必须执行DPIA的三种情况之一。（文献：A，第5章；GDPR第35(3)(c)条）
Correct. The project demands systematic monitoring of a publicly accessible area on a large scale, and this is one of the three mandatory scenarios for performing a DPIA. (Literature: A, Chapter 5; GDPR Article 35(3)(c))

D) 错误。只要人们的权利和自由得到充分保护，就不禁止监控、监视和特征分析。
Incorrect. Monitoring, surveillance and profiling are not prohibited, as long as people's rights and freedoms are sufficiently protected.

24 / 40

数据保护官（DPO）在执行其任务时受到保密要求的约束。

而涉及到哪一方时DPO可**免除**保密义务以寻求建议?

Data protection officers (DPOs) are bound by secrecy or confidentiality concerning the performance of their tasks.

In relation to which party is the DPO **exempted** from this secrecy or confidentiality to seek advice?

A) 公司董事会
The board of directors of the company

B) 数据和隐私保护成员小组
The data protection and privacy network members team

C) 信息安全官（ISO）
The information security officer (ISO)

D) 监管机构
The supervisory authority

A) 错误。可接洽不意味着DPO应征求董事会成员的建议。DPO应履行独立角色。
Incorrect. Being easily accessible does not mean that the DPO should ask for advice of board members. The DPO should fulfill an independent role.

B) 错误。可接洽并不意味着DPO应征求数据隐私保护成员小组的建议。
Incorrect. Being easily accessible does not mean that the DPO should ask for advice of the Data Protection and Privacy Network members' team.

C) 错误。可接洽并不意味着DPO应征求ISO的建议。
Incorrect. Being easily accessible does not mean that the DPO should ask for advice of the ISO.

D) 正确。保密义务并不禁止DPO与监管机构联系并征求建议。（文献：A，第2章；GDPR第36条和第39(1)(e)条）
Correct. The obligation of secrecy and or confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. (Literature: A, Chapter 2; GDPR Article 36 and Article 39(1)(e))

25 / 40

数据保护影响评估（DPIA）是一种用于识别数据保护风险的手段，尤其是识别可能对自然人的权利和自由产生重大影响的风险。

为什么DPIA可以被视为更宽泛的组织风险管理工作中的一部分？

A data protection impact assessment (DPIA) is a tool to identify data protection risks, especially the ones which are likely to highly affect the rights and freedoms of natural persons.

Why can the DPIA be seen as part of an organization's wider risk management?

A) 因为DPIA会评估受审组织的所有安全风险，并取代任何其他风险评估或风险管理
Because the DPIA assesses all security risks of the organization under review and replaces any other risk assessment or risk management

B) 因为DPIA通过风险的可能性和严重性来评估风险，类似于风险管理明确定义的其他组成部分
Because the DPIA assesses risks by the likelihood and severity of the risk, similar to other well-defined components of risk management

C) 因为根据GDPR，每个项目都必须执行DPIA，从而减少风对险管理的其他法律要求
Because the DPIA is mandatory for each project, according to the GDPR, which reduces all other legal requirements for risk management

A) 错误。DPIA仅关注个人数据和隐私保护风险。
Incorrect. A DPIA only focuses on personal data protection and privacy risks.

B) 正确。这是DPIA与风险管理之间的联系。（文献：A，第2章；GDPR序言第90条）
Correct. This is the link between DPIA and risk management. (Literature: A, Chapter 2; GDPR Recital 90)

C) 错误。DPIA并非总是必需的，而且它不会减少对其他风险管理的需求。
Incorrect. A DPIA is not always required and it does not diminish needs for other risk management.

26 / 40

根据GDPR，什么应始终是数据保护影响评估（DPIA）中的一个环节？

According to the GDPR, what should always be part of a data protection impact assessment (DPIA)?

A) 制定一个数据主体查阅请求的程序，以确保遵从数据主体的权利
Develop a subject access request procedure to ensure compliance with data subjects' rights

B) 明确已处理的个人数据以及处理的预期目的
Identify the personal data that are processed and the intended purposes of the processing

C) 通知数据主体将进行评估并征得其明确同意
Notify the data subjects that an assessment will take place and request their explicit consent

D) 制定事故响应计划并定义适当的防护措施，以避免数据泄露
Set up an incident response plan and define appropriate safeguards to avoid data breaches

A) 错误。根据DPIA的结果，这是一种可能的措施。
Incorrect. This is a possible measure, based on the outcome of a DPIA.

B) 正确。每次DPIA都应从对预期处理及其目的的描述着手。（文献：A，第8章；GDPR，第35(7)(a)条）
Correct. Every DPIA should start with a description of the intended processing and the purposes of the processing. (Literature: A, Chapter 8; GDPR, Article 35(7)(a))

C) 错误。执行DPIA不需要征得同意。
Incorrect. Consent is not required to do a DPIA.

D) 错误。根据DPIA的结果，这是一种可能的措施。
Incorrect. This is a possible measure, based on the outcome of a DPIA.

27 / 40

某组织开发一款新产品，用于发现表现不佳的员工。他们搜索员工的上网历史记录并使用人工智能（AI）分析其工作行为。

尽管软件工程师并不完全理解算法，但是管理层还是决定解雇表现垫底的10%员工。

数据保护官（DPO）对此产品的影响表示担忧，告知董事会需要执行一个数据保护影响评估（DPIA）。

什么**不是**此例必须执行DPIA的原因?

An organization develops a new product to find underperforming employees. They search their internet history and analyze work behavior using artificial intelligence (AI).

Although the software engineers do not fully understand the algorithm, management decides to fire the bottom 10% employees.

The data protection officer (DPO) is concerned about the impact of this product and informs the board that a data protection impact assessment (DPIA) is required.

What is **not** part of the reason why a DPIA is mandatory?

A) 个人数据处理的自动化
The automation of the personal data processing

B) 该评估可能显著影响数据主体
The evaluation that may affect the data subjects significantly

C) 处理特殊类别的个人数据
The processing of special categories of personal data

D) 系统评估自然人的个人方面
The systematic evaluation of personal aspects of natural persons

（题目未完，接下一页）

A) 错误。这是必须执行DPIA的原因。
Incorrect. This is a reason for a DPIA being mandatory.

B) 错误。这是必须执行DPIA的原因。
Incorrect. This is a reason for a DPIA being mandatory.

C) 正确。当系统将收集个人数据时，这些数据不被视为特殊类别的数据。（文献：A，第8章；GDPR第35条）
Correct. While the system will be collecting personal data, these data are not considered special categories of data. (Literature: A, Chapter 8; GDPR Article 35)

D) 错误。这是必须执行DPIA的原因。
Incorrect. This is a reason for a DPIA being mandatory.

28 / 40

什么**不属于**数据保护影响评估（DPIA）的产出?

What is **not** an outcome of a data protection impact assessment (DPIA)?

A) 带有自动化授权检查的机密数据查阅日志
A log of access to confidential data, with an automated authorization check

B) 数据主体对预期处理工作的看法的记录
A record of data subjects' views on the intended processing operations

C) 对预期处理工作的系统描述
A systematic description of the intended processing operations

D) 评估对数据主体权利和自由造成的风险
An assessment of risks to the rights and freedoms of data subjects

A) 正确。这不是DPIA的产出，而是信息安全部门持续进行的一项活动。（文献：A，第8章和第3章；GDPR第35条）
Correct. This is not an outcome of a DPIA, but is an ongoing activity performed by information security. (Literature: A, Chapter 8 and Chapter 3; GDPR Article 35)

B) 错误。这是DPIA一个可能的产出。
Incorrect. This is a possible outcome of the DPIA.

C) 错误。这是DPIA一个可能的产出。
Incorrect. This is a possible outcome of the DPIA.

D) 错误。这是DPIA一个可能的产出。
Incorrect. This is a possible outcome of the DPIA.

29 / 40

GDPR详细说明了数据保护影响评估（DPIA）必须至少输出的内容。

什么**不属于**DPIA的强制要求的?

The GDPR details what the output of a data protection impact assessment (DPIA) must contain at a minimum.

What is **not** mandatory in a DPIA?

A) 描述处理工作及其目的
A description of the processing and its purposes

B) 评估处理工作相对于目的的必要性和相称性
An assessment of the necessity and proportionality of the processing operations in relation to the purposes

C) 评估对数据主体权利和自由造成的风险
An assessment of the risks to the rights and freedoms of data subjects

D) 监管机构的建议
The advice of the supervisory authority

A) 错误。这属于DPIA的强制性要求。
Incorrect. This is a mandatory part of the DPIA.

B) 错误。这属于DPIA的强制性要求。
Incorrect. This is a mandatory part of the DPIA.

C) 错误。这属于DPIA的强制性要求。
Incorrect. This is a mandatory part of the DPIA.

D) 正确。向监管机构咨询并非总是强制要求的，在DPIA中有关建议的日志也非强制。（文献：A，第5章；GDPR第35(7)条和第36(1)条）
Correct. It is not always mandatory to consult with the supervisory authority, and it is not mandatory to include a log of the advice in the DPIA. (Literature: A, Chapter 5; GDPR Article 35(7) and Article 36(1))

30 / 40

一项数据保护影响评估（DPIA）表明，预期的处理工作将涉及到收集超出预期目的所必需的个体客户数据。

根据GDPR，什么是**最**恰当的应对?

A data protection impact assessment (DPIA) shows that the intended processing involves collecting more data on individual customers than is necessary to achieve the intended purpose.

According to the GDPR, what is the **most** appropriate response?

A) 尽快将数据匿名
Anonymize the data as soon as possible

B) 推出培训和意识培养计划
Introduce a training and awareness program

C) 限制数据存储的时长
Limit the period of time for which the data is stored

D) 减少数据收集量
Reduce the amount of data collected

A) 错误。这是一种减轻风险的措施，但首先是不处理不必要的数据。
Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place.

B) 错误。这是一种减轻风险的措施，但首先是不处理不必要的数据。
Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place.

C) 错误。这是一种减轻风险的措施，但首先是不处理不必要的数据。
Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place

D) 正确。这实现了数据最小化原则，并降低了对数据主体造成的风险。（文献：A，第8章；GDPR第5(1)条）
Correct. This implements the principle of data minimization and reduces the risks for the data subjects. (Literature: A, Chapter 8; GDPR 5(1))

31 / 40

在开始数据保护影响评估（DPIA）之前，最好**先**做什么?

What is best done **first**, before starting a data protection impact assessment (DPIA)?

A) 确定应对已识别风险的措施
Determining measures to address the identified risks

B) 确定是否需要执行DPIA
Determining whether there is a need for a DPIA

C) 识别对数据主体权利和自由造成的风险
Identifying the risks to the rights and freedoms of data subjects

A) 错误。这是DPIA的一部分，在确定是否需要做DPIA之后才进行。
Incorrect. This is part of a DPIA and done after determining the need for one.

B) 正确。组织需要确定法律是否要求执行DPIA或组织是否有执行一个DPIA的需求。（文献：A，第5章；GDPR第35(7)条）
Correct. The organization needs to determine whether the law requires a DPIA or if the needs of the organization demand one. (Literature: A, Chapter 5; GDPR Article 35(7))

C) 错误。这是DPIA的一部分，在确定是否需要做DPIA之后才进行。
Incorrect. This is part of a DPIA and done after determining the need for one.

32 / 40

某公司执行了一个数据保护影响评估（DPIA）。

为什么说绘制数据地图对其做DPIA有用?

A company performs a data protection impact assessment (DPIA).

Why is data mapping useful for a DPIA?

A) 它有助于评估所有隐私方面的组织风险。
It assesses all organizational risks to privacy.

B) 它有助于获得一个对使用中的个人数据的概览。
It helps to gain an overview of the personal data in use.

C) 它有助于告知所有相关方。
It helps to inform all relevant parties.

A) 错误。绘制数据地图并不评估风险。
Incorrect. Data mapping does not assess risks.

B) 正确。绘制数据地图可以识别使用中的数据。绘制数据流有助于识别必须评估的潜在风险。（文献：A，第7章）
Correct. Data mapping identifies data in use. Mapped data flows help to identify potential risks that must be assessed. (Literature: A, Chapter 7)

C) 错误。绘制数据地图不用于通知各方。
Incorrect. Data mapping is not used to inform parties.

33 / 40

某组织聘请了一名隐私专家。该组织希望将部分数据处理活动外包。该专家对涉及一个数据处理者来做处理工作进行一项数据保护影响评估（DPIA）。

DPIA中一个主要的步骤中要求由控制者来给出所有意见，而不要求处理者参与。

该步骤具体指哪一步?

A privacy expert is hired by an organization. They wish to outsource part of their data processing activities. The expert performs a data protection impact assessment (DPIA) on the processing that involves a data processor.

One of the main steps of a DPIA requires the controller to provide all the input and does not require the processor to be involved.

Which step is that?

A) 评估处理的必要性和相称性
Assessment of the necessity and proportionality of the processing

B) 评估对数据主体权利和自由造成的风险
Assessment of the risks to the rights and freedoms of data subjects

C) 缓解风险的措施，包括保障措施
Mitigating measures to address the risks, including safeguards

D) 系统描述预期的处理工作
Systematic descriptions of the intended processing operations

A) 正确。这是控制者的职责，不涉及处理者。（文献：A，第12章）
Correct. This is the responsibility of the controller and does not involve the processor. (Literature: A, Chapter 12)

B) 错误。需要处理者发表有关潜在风险的意见。
Incorrect. Input is needed from the processor on potential risks.

C) 错误。需要处理者对采取的缓解措施的意见。
Incorrect. Input is needed on the mitigating measures taken by the processor.

D) 错误。为了进行完整描述，需要处理者发表的意见。
Incorrect. To make a full description, input from the processor is needed.

34 / 40

一家大公司出现财务困难。董事会希望员工提高工作效率。

董事会决定开始一项试验，以监控员工的上网活动，并通过分析数据了解可以提高效率之处，而被归为*效率低下*的员工可能会被解雇。

为什么在采用该新程序之前必须进行一个数据保护影响评估（DPIA）？

A large company is struggling financially. The board wants employees to work more efficiently.

The board starts an experiment in which the internet activities of the employees are monitored. The data are analyzed to see where more efficiency can be achieved. People categorized as *inefficient* might be dismissed.

Why must a data protection impact assessment (DPIA) be done before using the new procedure?

A) 因为大公司会有大量员工。所以，处理工作将是大规模的。
Because a large company has many employees. Therefore, the processing will be large scale.

B) 因为这是一次试验。新的处理活动和试验性的处理活动都需要执行DPIA。
Because it is an experiment. A DPIA is required for new and experimental processing activities.

C) 因为这是一次系统性的处理，且相关决定可能会相当程度地影响员工。
Because it is systematic processing. The decisions might significantly affect the employees.

A) 错误。大规模可能会产生影响，但其本身并不是判定标准。而公共场所大规模监控则是一个判定标准。但是，该公司不属于公共场所。
Incorrect. The large scale may be of influence but is not a criterion by its own. Large scale monitoring in a public space would be a criterion. However, the company is not a public space.

B) 错误。这与处理是实验性的还是常规的活动无关。
Incorrect. It is irrelevant whether it concerns an experiment or an ordinary processing activity.

C) 正确。这被定义为必须执行DPIA的三种情况之一。（文献：A，第5章；GDPR第35(3)(b)条）
Correct. This is defined as one of the three cases in which a DPIA is mandatory. (Literature: A, Chapter 5; GDPR Article 35(3)(b))

35 / 40

某组织计划基于特征分析对客户实行自动决策。

在此例中数据保护影响评估（DPIA）的哪一部分需要特别注意?

An organization plans to make automated decisions on its clients, based on profiling.

Which part of the data protection impact assessment (DPIA) needs extra attention?

A) 针对此处理活动执行DPIA的需求的评估
The assessment of the need to perform a DPIA in relation to this processing activity

B) 将要实施的保护数据主体权利的措施
The measures to protect the rights of the data subject that will be implemented

C) 保护个人数据免受数据主体请求的措施
The measures to secure the personal data from being requested by data subjects

D) 数据主体要求删除其数据后，用来数据擦除的程序
The procedures for data erasure after a data subject asks for their data to be removed

A) 错误。涉及自动决策（包括特征分析）的处理活动总是需要执行DPIA。
Incorrect. For processing activities involving automated decision making, including profiling, a DPIA is always required.

B) 正确。自动决策带来的风险需要特别注意。应细致描述如何缓解风险。缓解措施可以是加入人为干预。（文献：A，第5章；GDPR第35条）
Correct. The risks automated decision-making bring with them need special attention. How to mitigate the risk should be carefully described. A mitigation could be to allow human intervention. (Literature: A, Chapter 5; GDPR Article 35)

C) 错误。总体而言数据需要保护其安全，但不妨碍数据主体有查阅权。
Incorrect. Data need to be secured in general, but data subjects have the right of access.

D) 错误。这是DPIA的一部分，但如果涉及自动决策，它就还不是那个最应特别被关注的。
Incorrect. This is part of a DPIA, but it is not most appropriate for specific attention if automated decisions are made.

36 / 40

GDPR规定，组织必须设法防止个人数据泄露。因此，要快速识别可归类为个人数据泄露的事故。

根据GDPR，哪一项**不属于**个人数据泄露事故?

The GDPR states that organizations must seek ways to prevent personal data breaches. Therefore, it is important to quickly recognize incidents that can be classified as personal data breaches.

According to the GDPR, which incident is **not** a personal data breach?

A) 患者期望收到装有医疗设备的包裹，但是包裹却被送错地址。
A patient is expecting a package containing medical equipment, but it is delivered to the wrong address.

B) 在精神卫生诊所工作的一名雇员放错了一套患者档案而且无法追溯。
An employee working at a mental health clinic has misplaced a set of patient files that cannot be retraced.

C) 数据仓库因火灾或地震意外破坏了个人数据。
The accidental destruction of personal data by a fire or an earthquake in a data warehouse.

D) 未经授权披露了公司一个涉及计划收购的有关机密财务数据。
The unauthorized disclosure of a company's confidential financial data regarding an intended acquisition.

A) 错误。这属于涉及特殊类别个人数据的个人数据泄露事故。
Incorrect. This is a personal data breach involving special category personal data.

B) 错误。任何个人数据（尤其是特殊类别的个人数据）的意外丢失都被视为个人数据泄露。
Incorrect. The accidental loss of any personal data, and especially special category personal data, is also considered a personal data breach.

C) 错误。即使事故是由于自然灾害或不可抗力造成的，也必须将其视为个人数据泄露事故。
Incorrect. Even if the incident is caused by a natural disaster or force majeure, this must be considered a personal data breach.

D) 正确。这属于数据泄露事故，但不会对个人数据造成破坏。所以不属于个人数据泄露事故。（文献：A，第3章；GDPR第4(12)条）
Correct. This is a data breach, but no personal data are compromised. It is not a personal data breach. (Literature: A, Chapter 3; GDPR Article 4(12))

37 / 40

在什么情况下需要向监管机构上报个人数据泄露事故?

In which situation is it required to report a personal data breach to the supervisory authority?

A) 组织在事故发生后72小时内无法解决
If the organization cannot resolve the incident within a timeframe of 72 hours after it has occurred

B) 在对自然人的权利和自由构成安全威胁的任何情况下
In any situation where there is a security threat to the rights and freedom of natural persons

C) 只要在72小时内将事故确认为个人数据泄露事故
Only if the incident is recognized as a personal data breach within a timeframe of 72 hours

D) 个人数据泄露可能给自然人的权利和自由带来风险时
When a personal data breach is likely to result in a risk to the rights and freedom of natural persons

A) 错误。解决事故的时间周期在这里并不重要。
Incorrect. The timeframe in which the incident is resolved is unimportant.

B) 错误。仅仅威胁还不足够。仅在发生个人数据泄露事故且可能给自然人的权利和自由带来风险时通知才是必需的。
Incorrect. A threat is not enough. A notification is only mandatory when a personal data breach occurred, that is likely to result in a risk to the rights and freedoms of natural persons.

C) 错误。事故管理流程可能无法在72小时内识别出事故。GDPR规定，必须"不得无故拖延，且在可行的情况下，在知悉后不迟于72小时内"报告个人数据泄露事故。
Incorrect. The incident management process may be unable to identify the incident within 72 hours. The GDPR states that personal data breaches must be reported "without undue delay and where feasible not later than 72 hours after having become aware of it".

D) 正确。对于涉及个人数据的事故，若可能给自然人的权利和自由带来风险，则必须通知监管机构。（文献：A，第14章；GDPR第33(1)条）
Correct. Notification to the supervisory authority is mandatory for incidents involving personal data, that are likely to result in a risk to the rights and freedoms of natural persons. (Literature: A, Chapter 14; GDPR Article 33(1))

38 / 40

人力资源（HR）部主管丢失了一个存储卡，其中包含35名员工的个人信息。该存储卡有强加密的保护。人力资源部曾将这些个人信息存储在备份设备中。

根据GDPR，是否必须将这一个人数据泄露事故上报给监管机构?

The head of the Human Resources (HR) department has lost a memory stick containing the personal information of 35 employees. The memory stick is protected by strong encryption. The HR department also has this personal information stored in a backup device.

According to the GDPR, is it mandatory to report this personal data breach to the supervisory authority?

A) 是，因为所有安全事件都必须上报给监管机构。
Yes, because all security incidents must be reported to the supervisory authority.

B) 是，因为报告监管机构后可以让其通知员工。
Yes, because reporting it enables the supervisory authority to inform the employees.

C) 否，因为报告数据泄露不符合公司的合法利益。
No, because it is not a legitimate interest of the company to report data breaches.

D) 否，因为该个人数据泄露事故不会对数据主体的权利造成风险。
No, because this personal data breach creates no risk to the data subjects' rights.

（题目未完，接下一页）

A) 错误。对数据主体权利造成高风险的个人数据泄露事故才必须上报。尽管上报所有个人数据泄露事件是避免违法的一种好做法，但这并不是强制性的。
Incorrect. Only personal data breaches that result in a high risk to the rights of data subject must be reported. Although it can be good practice to report all personal data breaches to avoid breaking the law, this is not mandatory.

B) 错误。数据主体的权利没有处于危险，因此无需通知他们。通知数据主体并非是监管机构的任务。
Incorrect. The data subjects' rights are not at risk, so they do not need to be informed. It is not the supervisory authority's task to inform the data subjects.

C) 错误。公司的合法利益是进行处理的法律基础。它与个人数据泄露以及如何上报无关。
Incorrect. The legitimate interest of the company is a legal ground for processing. It does not relate to personal data breaches and how these must be reported.

D) 正确。强加密和备份足以保证个人数据的机密性和可用性。因此，该数据泄露事故不太可能给自然人的权利和自由带来风险。所以上报该数据泄露事故给监管机构并非强制性要求。（文献：A，第14章；GDPR第33(1)条）
Correct. The strong encryption and backup are enough to guarantee the confidentiality and availability of the personal data. Therefore, this data breach is unlikely to result in a risk to the rights and freedoms of natural persons. It is not mandatory to report this data breach to the supervisory authority. (Literature: A, Chapter 14; GDPR Article 33(1))

39 / 40

根据GDPR，在什么情况下必须将个人数据泄露事故报告给受影响的数据主体?

According to the GDPR, in which situation must a personal data breach be reported to the data subjects affected?

A) 个人数据泄露可能给数据主体的权利和自由带来高风险时
When a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject

B) 监管机构判定同意是处理的唯一法律依据时
When the supervisory authority has determined that consent was the only legal ground for processing

C) 当一个安全事故在72小时内被列为个人数据泄露事故时
When there is a security incident that is labelled as a personal data breach within 72 hours

D) 个人数据受到黑客或其他网络罪犯等外部因素的破坏时
When personal data is compromised by external factors such as hackers or other cyber criminals

A) 正确。如果个人数据泄露给数据主体的权利和自由带来高风险，应告知数据主体。（文献：A，第14章；GDPR第34(1)条）
Correct. Data subjects should be informed if the personal data breach poses a high risk to their rights and freedoms. (Literature: A, Chapter 14; GDPR Article 34(1))

B) 错误。只有构成高风险的个人数据泄露事故才必须报告给数据主体。
Incorrect. Only personal data breaches that pose a high risk must also be reported to the data subjects.

C) 错误。72小时是应将个人数据泄露事故报告给监管机构的时间期限。并非所有个人数据泄露事故都必须报告给数据主体。
Incorrect. The 72 hours are the timeframe within which the personal data breach should be reported to the supervisory authority. Not all personal data breaches must be reported to the data subjects.

D) 错误。通知与否不取决于个人数据泄露的底层原因。
Incorrect. Notification does not depend on the underlying cause of the personal data breach.

40 / 40

在事故响应的最佳实践中定义了准备、响应和跟进几个阶段。每个阶段都必须进行存档。

在响应阶段，重要的是收集和保存证据，证明事件发生的原因以及组织未能防止事故发生的原因。

其中具体必须收集和保存是哪一个?

In the best practice incident response process the phases prepare, respond and follow-up are defined. For each phase, documentation is essential.

In the respond phase, it is important to gather and preserve evidence to show why an incident happened and why the organization was not able to prevent the incident.

What must be gathered and preserved?

A) 审计控制计划
Audit control plans

B) 数据保护影响评估（DPIAs）
Data protection impact assessments (DPIAs)

C) 能提供清晰图景的证据
Evidence to provide a clear picture

D) 系统恢复计划
System recovery plans

A) 错误。审计控制计划不是在事故响应过程中做存档。
Incorrect. An audit control plan is not documented in the incident response process.

B) 错误。DPIA不是在事故响应过程中做存档。
Incorrect. A DPIA is not documented in the incident response process.

C) 正确。在整个事故响应过程中，应收集并保存证据，以清楚地了解所发生的事情以及组织未能防止事故发生的原因。（文献：A，第14章）
Correct. Throughout the incident response process, evidence should be gathered and preserved to provide a clear picture of what happened and why the organization was unable to prevent the incident. (Literature: A, Chapter 14)

D) 错误。系统恢复计划不是在事故响应过程中做存档。
Incorrect. A system recovery plan is not documented in the incident response process.

试题评分

如下表格为本套样题的正确答案，供参考使用。

问题	答案	问题	答案
1	B	**21**	C
2	C	**22**	D
3	B	**23**	C
4	A	**24**	D
5	D	**25**	B
6	A	**26**	B
7	C	**27**	C
8	B	**28**	A
9	D	**29**	D
10	D	**30**	D
11	C	**31**	B
12	C	**32**	B
13	B	**33**	A
14	A	**34**	C
15	A	**35**	B
16	D	**36**	D
17	B	**37**	D
18	A	**38**	D
19	B	**39**	A
20	B	**40**	C

联系 EXIN

www.exinchina.cn

info.china@exin.com

WeChat ID: EXINCH