Sample Exam

Edition 202607

Copyright © EXIN Holding B.V. 2026. All rights reserved.
EXIN® is a registered trademark of EXIN.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Content

Introduction	4
Sample exam	5
Answer key	18
Evaluation	40

Introduction

This is the EXIN Privacy & Data Protection Professional (PDPP.EN) sample exam. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is correct.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth 1 point. You need 26 points or more to pass the exam.

The time allowed for this exam is 120 minutes.

You are allowed to use [the case study / the exam literature / an additional resource] for this exam.

Good luck!

Sample exam

1 / 40
According to the GDPR, what information is **not** a mandatory part of a privacy policy?

A) Information about international transfers of personal data to a third country
B) Information about the identity and contact details of the controller
C) Information relating to data security measures in the organization
D) Information relating to retention periods and data subject's rights

2 / 40
The GDPR specifies data protection by design and by default. A good way to implement data protection by design and by default is by using a privacy-by-design approach.

What is the link between data protection by design and by default and the privacy-by-design approach?

A) Default privacy settings, which are part of the design, should be as privacy friendly as possible.
B) Personal data cannot be legally processed without the data subject giving their consent.
C) Privacy-by-design is becoming the default organizational approach, following implementation of the GDPR.

3 / 40
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 time to discuss data protection?

A) From the start of the project
B) During the implementation phase
C) When the project nears completion

4 / 40
An organization implements a 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) Internal issue, because the legal requirements directly impact the PIMS, which is an internal matter.
B) Internal issue, because the relevant factors are the contractors who must be seen as coworkers.
C) External issue, because the contractors operate outside the regular coworkers of the organization.
D) External issue, because the legal requirements are relevant but independent from the organization.

5 / 40
A business to consumer (B2C) organization implements a privacy information management system (PIMS).

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

- 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) External hard drive
B) Paper files
C) Server
D) USB drives

6 / 40
The ISO/IEC 27701 mentions a document that details which privacy information management system (PIMS) controls to manage risks are applied and which are not.

What specific document is this?

A) Internal audit report
B) PIMS applicability statement
C) PIMS control report
D) Statement of applicability (SoA)

7 / 40
One part of a privacy information management system (PIMS), is meant 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 part of the PIMS is this a description of?

A) Audit
B) Documentation
C) Management review
D) Statement of applicability (SoA)

8 / 40
A company has implemented a privacy information management system (PIMS). The organization has determined that management reviews must be carried out every 12 months.

According to the ISO/IEC 27701, why is a management review **required**?

A) To confirm that all privacy risks have been sufficiently eliminated through the selection of privacy and security controls
B) To ensure the PIMS remains suitable, adequate, and effective in supporting the organization's privacy objectives
C) To review the agreed-upon operational procedures for handling personal data in the company
D) To verify that all processing activities fully comply with the GDPR in every case identified in the company

9 / 40
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) To assess whether working practices conform to the PIMS and its management system requirements
B) To evaluate whether third-party processors meet the organization's contractual privacy obligations
C) To provide assurance that no nonconformities or corrective actions remain open within the PIMS
D) To review whether the organization's privacy objectives remain aligned with its overall business strategy

10 / 40
An organization implements a privacy information management system (PIMS). The specific requirements must be based on local rules and contractual requirements.

What should the organization's legal team do to determine the specific requirements?

A) Hire local legal advice and guidance, and apply the ISO/IEC 27701 as the contractual standard to clients and suppliers
B) Look up the applicable international best practices, and review all contracts which involve personal data processing
C) Map the applicable legislation and related legal sanctions, and review all contracts which involve personal data processing
D) Request local supervisory authority's guidance, and apply the ISO/IEC 27701 as a contractual standard to clients and suppliers

11 / 40
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) A data protection impact assessment (DPIA) report
B) A privacy impact assessment (PIA) report
C) A recent PIMS audit report
D) A statement of applicability (SoA) report

12 / 40
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) The ISO/IEC 27701 certification of a supplier includes a cost/benefit analysis, which ensures lower costs for services.
B) The ISO/IEC 27701 certification of a supplier lowers the need for supplier audits, which is easier for the organization.
C) The ISO/IEC 27701 certification of the organization has procedures for data processing, which extends to any supplier.
D) The ISO/IEC 27701 certification of the organization requires an ISO/IEC 27701 certified supplier, which limits choices.

13 / 40
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) The ISMS and PIMS audits may be combined or done separately, even though the PIMS requirements depend on the maintenance of the ISMS.
B) The ISMS and PIMS audits must never be done together, because the PIMS and ISMS system requirements do not depend on each other.
C) The ISMS is part of the PIMS and addresses information protection, since the ISMS looks at a business risk approach to personal data.

14 / 40
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) The GDPR principles of integrity and confidentiality form the foundation of the PIMS that is required for the ISO/IEC 27701 standard.
B) The GDPR principles of lawfulness, fairness, and transparency contribute to the PIMS and the information security management system (ISMS).
C) The GDPR principle of purpose limitation prescribes exactly how the data that fall under the PIMS may or may not be used.
D) The GDPR principle of storage limitation explains the length of time the personal data reside in the PIMS before processing.

15 / 40
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) Develop privacy policies separate from or combined with information security policies
B) Ensure awareness training for all coworkers who handle or process personal data
C) Label data clearly to identify where personal data is stored or otherwise processed
D) Plan internal and external audits at specific intervals depending on the audit scope

16 / 40
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
B) 1, 3, 2
C) 2, 1, 3
D) 2, 3, 1

17 / 40
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) Because the contract determines this
B) Because the hospital is the controller
C) Because the mix-up is between patients
D) Because the verification has gone wrong

18 / 40
According to the GDPR, which activity is **always** a responsibility of the controller?

A) Being responsible for performing a data protection impact assessment (DPIA)
B) Contracting a security company for the protection of personal data in transit
C) Implementing a new method to collect personal data from the customers
D) Maintaining records of the processing activities carried out by the processor

19 / 40
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) When the processor contracts a company to protect data during transfers
B) When the processor contracts a third party to process personal data
C) When the processor implements a new method to collect personal data
D) When the processor implements a new method to delete personal data

20 / 40
Who has the legal obligation to keep records of processing activities?

A) The chief information officer
B) The chief privacy officer
C) The controller and processor
D) The data protection officer (DPO)

21 / 40
A North American organization processes personal data of natural persons based in the European Economic Area (EEA). 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) Foreigners' personal data are processed.
B) Personal data are processed in a third country.
C) Personal data of minorities are processed.
D) Special categories of personal data are processed on a large scale.

22 / 40
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) Ask the state secretary to contact the supervisory authority, because this is clearly outside the DPO's scope
B) Assure the state secretary that a data protection impact assessment (DPIA) is unnecessary, if data subjects are informed of the data processing
C) Inform the state secretary that a DPIA is mandatory for the large-scale monitoring of a public space
D) Urge the state secretary to reconsider the project because mass surveillance data processing is prohibited

23 / 40
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) The board of directors of the company
B) The data protection and privacy network members team
C) The information security officer (ISO)
D) The supervisory authority

24 / 40
A company performs a data protection impact assessment (DPIA).

According to the GDPR, what should **always** be part of a DPIA?

A) Develop a subject access request procedure to ensure compliance with data subjects' rights
B) Identify the personal data that are processed and the intended purposes of the processing
C) Notify the data subjects that an assessment will take place and request their explicit consent
D) Set up an incident response plan and define appropriate safeguards to avoid data breaches

25 / 40
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) The automation of the personal data processing
B) The evaluation that may affect the data subjects significantly
C) The processing of special categories of personal data
D) The systematic monitoring of personal aspects of natural persons

26 / 40
The GDPR requires a systematic description of the intended processing operations as a first outcome of a data protection impact assessment (DPIA).

What does this description help to do?

A) Check whether the processing is necessary to achieve the purpose
B) Get an overview of the systems and applications used by the organization
C) Identify the risks for the organization resulting from the processing
D) Review what the legitimate purpose for the intended processing is

27 / 40
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) Anonymize the data as soon as possible
B) Introduce a training and awareness program
C) Limit the period of time for which the data is stored
D) Reduce the amount of data collected

28 / 40
A company performs a data protection impact assessment (DPIA).

Why is **data mapping** useful for a DPIA?

A) It assesses all organizational risks to privacy.
B) It helps to gain an overview of the personal data in use.
C) It helps to inform all relevant parties.

29 / 40
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) Assessment of the necessity and proportionality of the processing
B) Assessment of the risks to the rights and freedoms of data subjects
C) Mitigating measures to address the risks, including safeguards
D) Systematic descriptions of the intended processing operations

30 / 40
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) The assessment of the need to perform a DPIA in relation to this processing activity
B) The measures to protect the rights of the data subject that will be implemented
C) The measures to secure the personal data from being requested by data subjects
D) The procedures for data erasure after a data subject asks for their data to be removed

31 / 40
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) Because a large company has many employees. Therefore, the processing will be large scale.
B) Because it is an experiment. A DPIA is required for new and experimental processing activities.
C) Because it is systematic processing. The decisions might significantly affect the employees.

32 / 40
An HR staff member drives home after work and ends up in a traffic jam. He decides to stop to buy some cat food, parks his car and leaves his laptop in the car. When he returns, the car window is broken, and the laptop has gone.

The incident is reported in the incident management system. The laptop contains all passwords to the personal data systems of current and previous staff in the organization. The laptop has strong encryption, which makes it highly unlikely that the data can be accessed.

According to the GDPR, which actions **must** be taken?

A) - Notify the supervisory authority
- Notify all current and previous staff

B) - Notify the supervisory authority
- Do not notify current and recent staff

C) - Do not notify the supervisory authority
- Do not notify the current and recent staff

33 / 40
In which situation is it required to report a personal data breach to the supervisory authority?

A) If the organization cannot resolve the incident within a timeframe of 72 hours after it has occurred
B) In any situation where there is a security threat to the rights and freedom of natural persons
C) Only if the incident is recognized as a personal data breach within a timeframe of 72 hours
D) When a personal data breach is likely to result in a risk to the rights and freedom of natural persons

34 / 40
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) Yes, because all security incidents must be reported to the supervisory authority.
B) Yes, because reporting it enables the supervisory authority to inform the employees.
C) No, because it is not a legitimate interest of the company to report data breaches.
D) No, because this personal data breach creates no risk to the data subjects' rights.

35 / 40
A large government institution has recently designated a data protection officer (DPO). One of the first activities of this DPO is defining the incident response process for personal data breaches.

The DPO discusses the impact on the current incident management process with the chief information security officer (CISO). The CISO suggests a standard reporting template to notify data subjects of a personal data breach.

What should the response of the DPO be?

A) The DPO agrees, because ISO/IEC 27001 requires a standard notification template.
B) The DPO agrees, because parts of the notification can be the same for all data subjects.
C) The DPO disagrees, because a standard notification template is not possible.
D) The DPO disagrees, because the notification depends on the number of data subjects.

36 / 40
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) Audit control plans
B) Data protection impact assessments (DPIAs)
C) Evidence to provide a clear picture
D) System recovery plans

37 / 40
Amara is a data protection officer at an insurance company that uses an AI system to calculate car insurance premiums. The system analyses personal data such as driving history, location, and age to determine the premium for each customer. When a customer asks why their premium is higher than expected, the company is unable to provide a meaningful explanation of how the AI system reached its calculation.

The company must comply with both the GDPR and the AI Act.

Which part of **GDPR** compliance is challenged **most** in this scenario?

A) Accountability, because the company cannot demonstrate that it has implemented appropriate security measures to protect against hackers.
B) Data minimization, because the AI system processes a wider range of personal data than is necessary to calculate an insurance premium.
C) Data subject rights, because the customer cannot fully exercise their right to an explanation of how the AI system used their personal data.
D) Storage limitation, because the AI system retains personal data beyond the period necessary for the purpose of calculating the insurance premium.

38 / 40
A large insurance company uses an AI system to process increasing numbers of high-value insurance claims. The human reviewers of the claims complain that the administrative workload also keeps increasing. The AI system has a strong accuracy record. A human reviewer has agreed with the AI assessment for 99% of the cases over the last 24 months. To improve efficiency, the company does the following:

- They will now allow the AI system to automatically approve or reject the claims without human review.
- They will process lower-value insurance claims using the same AI system from now on too.
- They will rely on additional personal data already on file to improve the accuracy of predictions further.
- They will rely on the e-mail address on file as additional information to send the decision to the customer.

The company must comply with both the GDPR and the AI Act.

Which part of **GDPR** compliance is challenged **most** in this scenario?

A) Allowing the AI system to automatically approve the claims, because this undermines accountability.
B) Processing lower-value insurance claims with AI, because there is no valid legal basis for the processing.
C) Relying on additional personal data for assessments, because this will breach data minimization.
D) Using the e-mail addresses on file, because this changes the original purpose of the e-mail addresses.

39 / 40
A data engineer at a retail company builds an AI recommendation engine that collects customers' browsing history, purchase records, location data, and social media activity. The data are used to predict which products a customer might buy next. The system stores all collected data indefinitely to improve future model performance in an encrypted database.

The company must comply with both the GDPR and the AI Act.

Which part of **GDPR** compliance is challenged **most** in this scenario?

A) Accountability, because the company does not document which customers and employees have access to the collected data.
B) Data minimization, because the system collects more personal data than necessary for predicting future product interests.
C) Data portability, because customers cannot transfer their data to another service provider easily due to the encryption used.
D) Purpose limitation, because the data collected for product recommendations is also stored to improve future model performance.

40 / 40
A compliance manager at a financial institution uses an AI system to assess loan applications. The system assigns credit scores based on historical financial data. A review reveals that the system consistently gives lower scores to applicants from certain demographic groups.

How do the AI Act requirements help to make sure that the GDPR principle of fairness is maintained in this scenario?

A) By focusing on preventing biased outcomes that could disadvantage certain groups through specific requirements for high-risk AI systems
B) By granting the financial institution the authority to define which demographic groups are excluded from the loan assessment process
C) By mandating that the financial institution publishes the full source code of the AI system used for credit scoring
D) By requiring the financial institution to replace the AI system with a manual review process for all loan applications

Answer key

1 / 40
According to the GDPR, what information is **not** a mandatory part of a privacy policy?

A) Information about international transfers of personal data to a third country
B) Information about the identity and contact details of the controller
C) Information relating to data security measures in the organization
D) Information relating to retention periods and data subject's rights

A) Incorrect. This is mandatory.
B) Incorrect. This is mandatory.
C) Correct. This is part of an information security policy. (Literature: A, Chapter 16; GDPR Article 13)
D) Incorrect. This is mandatory.

2 / 40
The GDPR specifies data protection by design and by default. A good way to implement data protection by design and by default is by using a privacy-by-design approach.

What is the link between data protection by design and by default and the privacy-by-design approach?

A) Default privacy settings, which are part of the design, should be as privacy friendly as possible.
B) Personal data cannot be legally processed without the data subject giving their consent.
C) Privacy-by-design is becoming the default organizational approach, following implementation of the GDPR.

A) Correct. For example, default settings are part of the design of a system or service. (Literature: A, Chapter 5; GDPR Article 25)
B) Incorrect. This is not the meaning nor a part of privacy by design either.
C) Incorrect. Privacy by default is one of the aspects of the privacy by design approach.

3 / 40
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 time to discuss data protection?

A) From the start of the project
B) During the implementation phase
C) When the project nears completion

A) 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) Incorrect. Discussing data protection in the implementation phase is too late.
C) Incorrect. Discussing data protection in the project completion phase is too late.

4 / 40
An organization implements a 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) Internal issue, because the legal requirements directly impact the PIMS, which is an internal matter.
B) Internal issue, because the relevant factors are the contractors who must be seen as coworkers.
C) External issue, because the contractors operate outside the regular coworkers of the organization.
D) External issue, because the legal requirements are relevant but independent from the organization.

A) Incorrect. Although the legal requirements will likely directly impact the PIMS, the legal requirements themselves are always external issues.
B) 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) 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) Correct. According to the term introduced by ISO/IEC 27701, legal requirements are considered external issues. (Literature: B, Chapter 2)

5 / 40
A business to consumer (B2C) organization implements a privacy information management system (PIMS).

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

- 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) External hard drive
B) Paper files
C) Server
D) USB drives

A) 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) 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) 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) Incorrect. All media that contain personal information should be part of the PIMS, even if the information is of former coworkers.

6 / 40
The ISO/IEC 27701 mentions a document that details which privacy information management system (PIMS) controls to manage risks are applied and which are not.

What specific document is this?

A) Internal audit report
B) PIMS applicability statement
C) PIMS control report
D) Statement of applicability (SoA)

A) Incorrect. It is the statement of applicability (SoA).
B) Incorrect. It is the statement of applicability (SoA).
C) Incorrect. It is the statement of applicability (SoA).
D) Correct. The statement of applicability (SoA) describes the control objectives and controls that are applicable and important to the organization's PIMS. (Literature: B, Chapter 4)

7 / 40
One part of a privacy information management system (PIMS), is meant 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 part of the PIMS is this a description of?

A) Audit
B) Documentation
C) Management review
D) Statement of applicability (SoA)

A) Incorrect. A management system audit program has the main objective to monitor conformity between the management system requirements and working practices.
B) 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) 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) Incorrect. The SoA is a document that details which controls are applied within the PIMS and which are not.

8 / 40
A company has implemented a privacy information management system (PIMS). The organization has determined that management reviews must be carried out every 12 months.

According to the ISO/IEC 27701, why is a management review **required**?

A) To confirm that all privacy risks have been sufficiently eliminated through the selection of privacy and security controls
B) To ensure the PIMS remains suitable, adequate, and effective in supporting the organization's privacy objectives
C) To review the agreed-upon operational procedures for handling personal data in the company
D) To verify that all processing activities fully comply with the GDPR in every case identified in the company

A) Incorrect. Management review is not intended to confirm that all privacy risks have been eliminated through controls. Risk treatment reduces risks to acceptable levels, but management review evaluates the overall performance of the PIMS.
B) Correct. A management review is required to ensure that the PIMS remains suitable, adequate, and effective in supporting the organization's privacy objectives. Under ISO/IEC 27701, top management must ensure that such reviews take place at planned intervals. (Literature: B, Chapter 3)
C) Incorrect. Management review is not required to review detailed operational procedures for handling personal data. It is a higher-level activity focused on the overall performance and continued suitability of the PIMS.
D) Incorrect. Management review is not required to verify that all processing activities fully comply with the GDPR in every case. Compliance is relevant, but the main purpose of the review is to assess whether the PIMS remains suitable, adequate, and effective.

9 / 40
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) To assess whether working practices conform to the PIMS and its management system requirements
B) To evaluate whether third-party processors meet the organization's contractual privacy obligations
C) To provide assurance that no nonconformities or corrective actions remain open within the PIMS
D) To review whether the organization's privacy objectives remain aligned with its overall business strategy

A) Correct. Audits mainly verify that actual practices match PIMS requirements. (Literature: B, Chapter 3)
B) Incorrect. This is only one possible area of review, not the main audit objective.
C) Incorrect. Audits may review these, but their main purpose is to assess conformity.
D) Incorrect. This is mainly part of management review, not auditing.

10 / 40
An organization implements a privacy information management system (PIMS). The specific requirements must be based on local rules and contractual requirements.

What should the organization's legal team do to determine the specific requirements?

A) Hire local legal advice and guidance, and apply the ISO/IEC 27701 as the contractual standard to clients and suppliers
B) Look up the applicable international best practices, and review all contracts which involve personal data processing
C) Map the applicable legislation and related legal sanctions, and review all contracts which involve personal data processing
D) Request local supervisory authority's guidance, and apply the ISO/IEC 27701 as a contractual standard to clients and suppliers

A) Incorrect. Local legal advice may help, but it is not always necessary if the legal team already understands the applicable laws. Also, ISO/IEC 27701 does not need to be included as a contractual standard in all contracts.
B) Incorrect. The specific requirements of a PIMS must be determined considering contractual requirements and the applicable local legislation, not international best practices.
C) Correct. The organization should identify the applicable local legal requirements, including sanctions, and review contracts involving personal data processing to determine PIMS requirements. (Literature: B, Chapter 4)
D) Incorrect. Supervisory authority guidance is not required to determine the requirements, and ISO/IEC 27701 does not need to be imposed as a contractual standard in all contracts.

11 / 40
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) A data protection impact assessment (DPIA) report
B) A privacy impact assessment (PIA) report
C) A recent PIMS audit report
D) A statement of applicability (SoA) report

A) 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) 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) Correct. Audit reports identify conformity and non-conformity between the actual practice and the requirements. (Literature: B, Chapter 3)
D) 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.

12 / 40
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) The ISO/IEC 27701 certification of a supplier includes a cost/benefit analysis, which ensures lower costs for services.
B) The ISO/IEC 27701 certification of a supplier lowers the need for supplier audits, which is easier for the organization.
C) The ISO/IEC 27701 certification of the organization has procedures for data processing, which extends to any supplier.
D) The ISO/IEC 27701 certification of the organization requires an ISO/IEC 27701 certified supplier, which limits choices.

A) 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) 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) 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) 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.

13 / 40
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) The ISMS and PIMS audits may be combined or done separately, even though the PIMS requirements depend on the maintenance of the ISMS.
B) The ISMS and PIMS audits must never be done together, because the PIMS and ISMS system requirements do not depend on each other.
C) The ISMS is part of the PIMS and addresses information protection, since the ISMS looks at a business risk approach to personal data.

A) 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) 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) 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.

14 / 40
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) The GDPR principles of integrity and confidentiality form the foundation of the PIMS that is required for the ISO/IEC 27701 standard.
B) The GDPR principles of lawfulness, fairness, and transparency contribute to the PIMS and the information security management system (ISMS).
C) The GDPR principle of purpose limitation prescribes exactly how the data that fall under the PIMS may or may not be used.
D) The GDPR principle of storage limitation explains the length of time the personal data reside in the PIMS before processing.

A) 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) 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) 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) 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.

15 / 40
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) Develop privacy policies separate from or combined with information security policies
B) Ensure awareness training for all coworkers who handle or process personal data
C) Label data clearly to identify where personal data is stored or otherwise processed
D) Plan internal and external audits at specific intervals depending on the audit scope

A) Incorrect. The recommendation to develop privacy policies is a part of this chapter.
B) Incorrect. The recommendation to ensure at least some training is in this chapter.
C) Incorrect. The recommendation to label all data clearly is part of this chapter.
D) 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)

16 / 40
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
B) 1, 3, 2
C) 2, 1, 3
D) 2, 3, 1

A) Incorrect. The correct order is 1, 3, 2.
B) 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) Incorrect. The correct order is 1, 3, 2.
D) Incorrect. The correct order is 1, 3, 2.

17 / 40
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) Because the contract determines this
B) Because the hospital is the controller
C) Because the mix-up is between patients
D) Because the verification has gone wrong

A) Incorrect. The hospital is accountable because, as the controller, it is subject to the accountability principle, determined by the GDPR.
B) 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) Incorrect. It does not matter that the data subjects all belong to the same controller. Who is the controller is relevant here.
D) Incorrect. There is nothing to indicate the verification went wrong. The supervisory authority will always hold the controller responsible.

18 / 40
According to the GDPR, which activity is **always** a responsibility of the controller?

A) Being responsible for performing a data protection impact assessment (DPIA)
B) Contracting a security company for the protection of personal data in transit
C) Implementing a new method to collect personal data from the customers
D) Maintaining records of the processing activities carried out by the processor

A) 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) Incorrect. This could be the responsibility of the processor, if prior written authorization exists.
C) Incorrect. This could be the responsibility of the processor, if prior written authorization exists.
D) Incorrect. This element is the responsibility of the processor. The controller maintains a record of the processing activities they control.

19 / 40
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) When the processor contracts a company to protect data during transfers
B) When the processor contracts a third party to process personal data
C) When the processor implements a new method to collect personal data
D) When the processor implements a new method to delete personal data

A) 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) 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) 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) 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.

20 / 40
Who has the legal obligation to keep records of processing activities?

A) The chief information officer
B) The chief privacy officer
C) The controller and processor
D) The data protection officer (DPO)

A) Incorrect. The chief information officer has the overall responsibility for information technology and information management.
B) Incorrect. The chief privacy officer should create engagement for GDPR compliance within the organization.
C) Correct. Both controller and processor are required to keep a record of all processing activities. (Literature: A, Chapter 12; GDPR Article 30)
D) 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.

21 / 40
A North American organization processes personal data of natural persons based in the European Economic Area (EEA). 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) Foreigners' personal data are processed.
B) Personal data are processed in a third country.
C) Personal data of minorities are processed.
D) Special categories of personal data are processed on a large scale.

A) Incorrect. This is not one of the three basic conditions specified in the GDPR.
B) Incorrect. This is not one of the three basic conditions specified in the GDPR.
C) Incorrect. This is not one of the three basic conditions specified in the GDPR.
D) 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)

22 / 40
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) Ask the state secretary to contact the supervisory authority, because this is clearly outside the DPO's scope
B) Assure the state secretary that a data protection impact assessment (DPIA) is unnecessary, if data subjects are informed of the data processing
C) Inform the state secretary that a DPIA is mandatory for the large-scale monitoring of a public space
D) Urge the state secretary to reconsider the project because mass surveillance data processing is prohibited

A) Incorrect. A DPO should be sufficiently qualified to discuss this.
B) Incorrect. Informing data subjects will not exempt an organization from the responsibility to do a DPIA.
C) 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) Incorrect. Monitoring, surveillance and profiling are not prohibited, as long as people's rights and freedoms are sufficiently protected.

23 / 40
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) The board of directors of the company
B) The data protection and privacy network members team
C) The information security officer (ISO)
D) The supervisory authority

A) 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) Incorrect. Being easily accessible does not mean that the DPO should ask for advice of the data protection and privacy network members' team.
C) Incorrect. Being easily accessible does not mean that the DPO should ask for advice of the ISO.
D) 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))

24 / 40
A company performs a data protection impact assessment (DPIA).

According to the GDPR, what should **always** be part of a DPIA?

A) Develop a subject access request procedure to ensure compliance with data subjects' rights
B) Identify the personal data that are processed and the intended purposes of the processing
C) Notify the data subjects that an assessment will take place and request their explicit consent
D) Set up an incident response plan and define appropriate safeguards to avoid data breaches

A) Incorrect. This is a possible measure, based on the outcome of a DPIA.
B) 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) Incorrect. Consent is not required to do a DPIA.
D) Incorrect. This is a possible measure, based on the outcome of a DPIA.

25 / 40
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) The automation of the personal data processing
B) The evaluation that may affect the data subjects significantly
C) The processing of special categories of personal data
D) The systematic monitoring of personal aspects of natural persons

A) Incorrect. This is a reason for a DPIA being mandatory.
B) Incorrect. This is a reason for a DPIA being mandatory.
C) 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) Incorrect. This is a reason for a DPIA being mandatory.

26 / 40
The GDPR requires a systematic description of the intended processing operations as a first outcome of a data protection impact assessment (DPIA).

What does this description help to do?

A) Check whether the processing is necessary to achieve the purpose
B) Get an overview of the systems and applications used by the organization
C) Identify the risks for the organization resulting from the processing
D) Review what the legitimate purpose for the intended processing is

A) Correct. This is to fulfill the requirement of purpose limitation, which is the background for the processing. (Literature: A, Chapter 8; GDPR Article 35(7))
B) Incorrect. This overview is required by Article 30 from the GDPR but cannot be achieved by a DPIA.
C) Incorrect. Risks for the organization are not part of a DPIA.
D) Incorrect. The legitimate purpose for the processing must have been identified from the start.

27 / 40
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) Anonymize the data as soon as possible
B) Introduce a training and awareness program
C) Limit the period of time for which the data is stored
D) Reduce the amount of data collected

A) Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place.
B) Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place.
C) Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place
D) Correct. This implements the principle of data minimization and reduces the risks for the data subjects. (Literature: A, Chapter 8; GDPR 5(1))

28 / 40
A company performs a data protection impact assessment (DPIA).

Why is **data mapping** useful for a DPIA?

A) It assesses all organizational risks to privacy.
B) It helps to gain an overview of the personal data in use.
C) It helps to inform all relevant parties.

A) Incorrect. Data mapping does not assess risks.
B) Correct. Data mapping identifies data in use. Mapped data flows help to identify potential risks that must be assessed. (Literature: A, Chapter 7)
C) Incorrect. Data mapping is not used to inform parties.

29 / 40
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) Assessment of the necessity and proportionality of the processing
B) Assessment of the risks to the rights and freedoms of data subjects
C) Mitigating measures to address the risks, including safeguards
D) Systematic descriptions of the intended processing operations

A) Correct. This is the responsibility of the controller and does not involve the processor. (Literature: A, Chapter 12)
B) Incorrect. Input is needed from the processor on potential risks.
C) Incorrect. Input is needed on the mitigating measures taken by the processor.
D) Incorrect. To make a full description, input from the processor is needed.

30 / 40
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) The assessment of the need to perform a DPIA in relation to this processing activity
B) The measures to protect the rights of the data subject that will be implemented
C) The measures to secure the personal data from being requested by data subjects
D) The procedures for data erasure after a data subject asks for their data to be removed

A) Incorrect. For processing activities involving automated decision making, including profiling, a DPIA is always required.
B) Correct. The risks automated decision-making brings with it 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) Incorrect. Data need to be secured in general, but data subjects have the right of access.
D) Incorrect. This is part of a DPIA, but it is not most appropriate for specific attention if automated decisions are made.

31 / 40
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) Because a large company has many employees. Therefore, the processing will be large scale.
B) Because it is an experiment. A DPIA is required for new and experimental processing activities.
C) Because it is systematic processing. The decisions might significantly affect the employees.

A) 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) Incorrect. It is irrelevant whether it concerns an experiment or an ordinary processing activity.
C) 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))

32 / 40
An HR staff member drives home after work and ends up in a traffic jam. He decides to stop to buy some cat food, parks his car and leaves his laptop in the car. When he returns, the car window is broken, and the laptop has gone.

The incident is reported in the incident management system. The laptop contains all passwords to the personal data systems of current and previous staff in the organization. The laptop has strong encryption, which makes it highly unlikely that the data can be accessed.

According to the GDPR, which actions **must** be taken?

A) - Notify the supervisory authority
- Notify all current and previous staff

B) - Notify the supervisory authority
- Do not notify current and recent staff

C) - Do not notify the supervisory authority
- Do not notify the current and recent staff

A) Incorrect. There is no need to notify the supervisory authority or the data subjects (current and previous staff), because the personal data breach is not likely to result in a risk to rights and freedoms of natural persons. The laptop's strong encryption ensures a low risk of unauthorized access.

B) Incorrect. There is no need to notify the supervisory authority or the data subjects (current and previous staff), because the personal data breach is not likely to result in a risk to rights and freedoms of natural persons. The laptop's strong encryption ensures a low risk of unauthorized access.

C) Correct. There is no need to notify the supervisory authority or the data subjects (current and previous staff), because the personal data breach is not likely to result in a risk to rights and freedoms of natural persons. The laptop's strong encryption ensures a low risk of unauthorized access. (Literature: A, Chapter 14; GDPR Article 33(1), Article 34(1) and Article (3)(a))

33 / 40
In which situation is it required to report a personal data breach to the supervisory authority?

A) If the organization cannot resolve the incident within a timeframe of 72 hours after it has occurred

B) In any situation where there is a security threat to the rights and freedom of natural persons

C) Only if the incident is recognized as a personal data breach within a timeframe of 72 hours

D) When a personal data breach is likely to result in a risk to the rights and freedom of natural persons

A) Incorrect. The timeframe in which the incident is resolved is unimportant.

B) 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) 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) 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))

34 / 40
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) Yes, because all security incidents must be reported to the supervisory authority.
B) Yes, because reporting it enables the supervisory authority to inform the employees.
C) No, because it is not a legitimate interest of the company to report data breaches.
D) No, because this personal data breach creates no risk to the data subjects' rights.

A) 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) 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) 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) 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))

35 / 40
A large government institution has recently designated a data protection officer (DPO). One of the first activities of this DPO is defining the incident response process for personal data breaches.

The DPO discusses the impact on the current incident management process with the chief information security officer (CISO). The CISO suggests a standard reporting template to notify data subjects of a personal data breach.

What should the response of the DPO be?

A) The DPO agrees, because ISO/IEC 27001 requires a standard notification template.
B) The DPO agrees, because parts of the notification can be the same for all data subjects.
C) The DPO disagrees, because a standard notification template is not possible.
D) The DPO disagrees, because the notification depends on the number of data subjects.

A) Incorrect. The ISO/IEC 27001 standard is irrelevant.
B) Correct. All notifications of data breaches to data subjects should always contain certain data, as described in the GDPR. A template helps ensure nothing is forgotten. Most parts of the notification will be the same for all data subjects. (Literature: GDPR, Article 33 and Article 34)
C) Incorrect. A template does not mean all information is prefilled. A template is possible and a good idea.
D) Incorrect. The number of the data subjects involved is irrelevant in this respect.

36 / 40
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) Audit control plans
B) Data protection impact assessments (DPIAs)
C) Evidence to provide a clear picture
D) System recovery plans

A) Incorrect. An audit control plan is not documented in the incident response process.
B) Incorrect. A DPIA is not documented in the incident response process.
C) 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) Incorrect. A system recovery plan is not documented in the incident response process.

37 / 40
Amara is a data protection officer at an insurance company that uses an AI system to calculate car insurance premiums. The system analyses personal data such as driving history, location, and age to determine the premium for each customer. When a customer asks why their premium is higher than expected, the company is unable to provide a meaningful explanation of how the AI system reached its calculation.

The company must comply with both the GDPR and the AI Act.

Which part of **GDPR** compliance is challenged **most** in this scenario?

A) Accountability, because the company cannot demonstrate that it has implemented appropriate security measures to protect against hackers.
B) Data minimization, because the AI system processes a wider range of personal data than is necessary to calculate an insurance premium.
C) Data subject rights, because the customer cannot fully exercise their right to an explanation of how the AI system used their personal data.
D) Storage limitation, because the AI system retains personal data beyond the period necessary for the purpose of calculating the insurance premium.

A) Incorrect. While accountability is a relevant GDPR principle, the core issue here is not the absence of security measures but the inability to explain how personal data was used to reach a specific outcome for the customer.
B) Incorrect. The scenario does not indicate that excessive data is being collected. The challenge described relates to the customer's inability to obtain an explanation of how their premium was calculated, not to the volume of data processed.
C) Correct. The AI Act entitles this customer to a clear explanation of how their premium is calculated. When a company is unable to provide this explanation, it directly undermines the customer's ability to exercise their data subject rights under GDPR. (Literature: C, Data Subject Rights)
D) Incorrect. The scenario does not raise any concern about how long personal data is retained. The challenge described is about the transparency of the AI system's calculation process, not about data retention periods.

38 / 40
A large insurance company uses an AI system to process increasing numbers of high-value insurance claims. The human reviewers of the claims complain that the administrative workload also keeps increasing. The AI system has a strong accuracy record. A human reviewer has agreed with the AI assessment for 99% of the cases over the last 24 months. To improve efficiency, the company does the following:

- They will now allow the AI system to automatically approve or reject the claims without human review.
- They will process lower-value insurance claims using the same AI system from now on too.
- They will rely on additional personal data already on file to improve the accuracy of predictions further.
- They will rely on the e-mail address on file as additional information to send the decision to the customer.

The company must comply with both the GDPR and the AI Act.

Which part of **GDPR** compliance is challenged **most** in this scenario?

A) Allowing the AI system to automatically approve the claims, because this undermines accountability.
B) Processing lower-value insurance claims with AI, because there is no valid legal basis for the processing.
C) Relying on additional personal data for assessments, because this will breach data minimization.
D) Using the e-mail addresses on file, because this changes the original purpose of the e-mail addresses.

A) Correct. GDPR accountability requires that organizations establish processes for human oversight in high-risk AI systems, including human intervention or approval for critical decisions. Removing human review from a high-value claims process directly undermines this requirement. (Literature: C, Accountability)
B) Incorrect. A claim with an insurer implies a contract (insurance policy). Therefore, there is indeed a legitimate basis for the processing (GDPR, Article 6.1(b))
C) Incorrect. Data minimization concerns the volume and relevance of data collected, not the absence of human oversight in the decision-making process. The scenario focuses on how decisions are made, not on what data is gathered.
D) Incorrect. Purpose limitation applies when data is used for a purpose other than the one originally specified. The scenario does not describe a change in the purpose of data use, but rather the lack of human control over critical AI-driven decisions.

39 / 40
A data engineer at a retail company builds an AI recommendation engine that collects customers' browsing history, purchase records, location data, and social media activity. The data are used to predict which products a customer might buy next. The system stores all collected data indefinitely to improve future model performance in an encrypted database.

The company must comply with both the GDPR and the AI Act.

Which part of **GDPR** compliance is challenged **most** in this scenario?

A) Accountability, because the company does not document which customers and employees have access to the collected data.
B) Data minimization, because the system collects more personal data than necessary for predicting future product interests.
C) Data portability, because customers cannot transfer their data to another service provider easily due to the encryption used.
D) Purpose limitation, because the data collected for product recommendations is also stored to improve future model performance.

A) Incorrect. Accountability concerns an organization's ability to demonstrate compliance with GDPR principles. The scenario highlights the volume and variety of data collected, not a lack of access documentation.
B) Correct. GDPR requires data minimization (art. 5.1.c), meaning only data that is adequate, relevant, and limited to what is necessary may be processed. Collecting browsing history, location data, and social media activity beyond what is needed to make product recommendations violates this principle. (Literature: C, Purpose limitation and data minimization).
C) Incorrect. Data portability relates to the right of individuals to receive their personal data in a structured format for transfer. The scenario does not describe any obstacle to moving data between service providers.
D) Incorrect. Using data for a secondary purpose such as model improvement may raise concerns, but the more prominent issue in this scenario is the excessive volume and variety of data types collected, which points to a different GDPR principle.

40 / 40
A compliance manager at a financial institution uses an AI system to assess loan applications. The system assigns credit scores based on historical financial data. A review reveals that the system consistently gives lower scores to applicants from certain demographic groups.

How do the AI Act requirements help to make sure that the GDPR principle of fairness is maintained in this scenario?

A) By focusing on preventing biased outcomes that could disadvantage certain groups through specific requirements for high-risk AI systems
B) By granting the financial institution the authority to define which demographic groups are excluded from the loan assessment process
C) By mandating that the financial institution publishes the full source code of the AI system used for credit scoring
D) By requiring the financial institution to replace the AI system with a manual review process for all loan applications

A) Correct. The AI Act includes specific requirements aimed at preventing biased outcomes that could disadvantage certain groups, which directly supports the GDPR principle of fairness. (Literature: C, User story: ensuring fairness)
B) Incorrect. The AI Act does not give organizations the authority to exclude demographic groups from AI-driven assessments, as this would contradict the goal of preventing discriminatory outcomes.
C) Incorrect. The AI Act does not require organizations to publish the full source code of their AI systems, as transparency obligations focus on documentation and human oversight instead.
D) Incorrect. The AI Act does not require organizations to replace AI systems with manual processes, but rather sets requirements to ensure AI systems operate fairly and without bias.

Evaluation

The table below shows the correct answers to the questions in this sample exam.

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

Certified for what's next

Contact EXIN

www.exin.com