Sample Exam

Edition 202508

Content

Introduction

This is the EXIN Privacy & Data Protection Foundation (PDPF.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 60 minutes.

Good luck!

Sample exam

1 / 40
What is the relationship between data protection and privacy?

A) Data protection and privacy are synonyms and have the same meaning.
B) Data protection is the part of privacy that protects a person's physical integrity.
C) Data protection refers to the measures needed to protect a person's privacy.

2 / 40
In the legal system of the European Union (EU), different tools are used to reach various goals. Some of these tools are binding, while others let EU Member States decide how to use them, offering them flexibility.

Does the GDPR allow this flexibility?

A) Yes, because it is a directive, which sets goals for EU Member States and sets out national measures.
B) Yes, because it is a recommendation that gives advice without further specific legal obligations.
C) No, because it is a decision that is binding only for specific parties and not for all EU Member States.
D) No, because it is a regulation, that applies to all EU Member States and is directly applicable.

3 / 40
How does the GDPR define personal data?

A) Any information relating to a resident of the European Economic Area (EEA)
B) Any information relating to an identified or identifiable natural person
C) Data that directly relate to an identified or identifiable natural person
D) Data that reveal someone's racial or ethnic background, religious views, health, sex life or sexual orientation

4 / 40
According to the GDPR, what is the definition of processing of personal data?

A) Any operation that can be performed on personal data
B) Any operation that can be performed on personal data, except erasing and destroying
C) Only operations in which the personal data is shared or transferred in any way
D) Only operations in which the personal data is used for the purposes for which it was collected

5 / 40
The GDPR defines some personal data as special category data, sometimes called 'sensitive data'.

What is an example of this type of data?

A) A collection of employees' work email addresses
B) A genealogical register of someone's ancestors
C) A list of payments made using a credit card
D) An address list of members of a political party

6 / 40
One of the roles described in the GDPR is defined as:

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Which role is defined here?

A) Controller
B) Processor
C) Supervisory authority
D) Third party

7 / 40
Processing of personal data must be lawful. A company collects personal data of its customers.

What is **always** necessary for lawful processing when collecting personal data?

A) Asking permission from the supervisory authority for the processing
B) Documenting a legitimate ground for the processing of the personal data
C) Implementing a code of conduct describing the nature of the processing

8 / 40
According to the GDPR, the controller must keep a record of all processing activities.

Which record is **not** obligatory according to the GDPR?

A) A record of all implemented technical and organizational measures of all processors
B) A record of all intended processing together with the processing purposes and legal justifications
C) A record of data breaches with all relevant characteristics, including notifications

9 / 40
One of the seven principles of data protection by design is *full functionality – positive-sum, not zero-sum*.

What is the essence of this principle?

A) Data protection coexists with security to create a win-win situation, which accomodates legitimate interests together with privacy.
B) Data protection includes informing data subjects about the ways their data is processed, which helps data subjects to stay in control.
C) Data protection is built into the architecture and design of the systems, which makes it a core functionality.

10 / 40
What is a description of data protection by design and by default?

A) An approach that implements data protection from development
B) An indication of timeframes if processing relates to erasure
C) Data may only be collected for explicit and legitimate purposes
D) Not holding more data than is strictly required for processing

11 / 40
To plan the amount of parking space needed, a local government monitors and saves the license plate number of every car that enters and leaves the city center. By comparing the license plate time of entry and exit the number of cars present every moment of each day is calculated.

They have obtained permission to collect data on the number of cars present in the city center. Each month a report is created detailing the average number of cars in the city center at specific moments for every day of the week.

At every entrance to the city center, a billboard clearly states what data is collected by whom, the purpose of the processing and the fact that the license plate numbers are saved securely for up to two years, because the measurements will be repeated next year.

Which of the basic principles for legitimate processing of personal data is **violated** in this scenario?

A) Personal data are collected for specified, explicit and legitimate purposes and not further processed.
B) Personal data are kept in a form permitting identification of data subjects for no longer than is necessary.
C) Personal data are processed in a manner that ensures appropriate security of the personal data.
D) Personal data are processed in a transparent manner in relation to the data subject.

12 / 40
Further processing, after the original objective is fulfilled, is allowed in a few specific cases, provided that appropriate safeguards for the rights and freedoms of the data subjects are taken.

For which purpose is further processing **not** allowed?

A) For archiving purposes in the public interest
B) For direct marketing and commercial purposes
C) For generalized statistical purposes
D) For scientific or historical research purposes

13 / 40
An organization provides its privacy notice in multiple languages and formats, including online, print, and audio, to ensure that all data subjects can access and understand it.

Which GDPR right does this practice support **most** directly?

A) The right to erasure, because data subjects are helped to understand that they have the right to delete their data any time.
B) The right to object, because data subjects can object to processing better when they understand the privacy notice completely.
C) The right to restriction, because data subjects are informed about the company's objectives and the legitimate grounds for processing.
D) The right to transparent information, communication, and modalities, because data subjects are helped to understand the privacy notice.

14 / 40
Which data subject right is explicitly defined by the GDPR?

A) A copy of personal data must be provided in the format requested by the data subject.
B) Access to personal data must be provided free of charge for the data subject.
C) Personal data must always be changed at the request of the data subject.
D) Personal data must always be erased if the data subject requests this.

15 / 40
A person buys a suit and provides the shop with his consent to use his e-mail address for advertising. Once the customer gets home, he asks the shop to erase all his personal data and stop sending him e-mails.

According to the GDPR, what must the shop do?

A) The shop may not delete any of his personal data since information about sales must be kept.
B) The shop must delete all personal data of this person for which the legitimate ground is consent.
C) The shop must delete his other personal data but can keep sending e-mails.

16 / 40
A person regularly receives offers from a store where he purchased something five years ago. He wants the company to stop sending offers and to delete his personal data.

Which of the data subjects' rights is he exercising?

A) The right of access
B) The right to object
C) The right to rectification
D) The right to restriction of processing

17 / 40
A company uses artificial intelligence (AI) to analyze job application letters and automatically decide to invite them for an interview.

Which GDPR right is **most** relevant to this scenario?

A) The right not to be subject to a decision based solely on automated processing
B) The right to lodge a complaint with a supervisory authority
C) The right to restriction of processing
D) The right to transparent information, communication, and modalities

18 / 40
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Which data processing principle is described here?

A) Accuracy
B) Data minimization
C) Lawfulness, fairness, and transparency
D) Purpose limitation

19 / 40
The GDPR describes the principle of data minimization.

How can organizations comply with this principle?

A) By applying the concept of least privilege to the personal data collected, stored or otherwise processed
B) By limiting access rights to staff who need the personal data for the intended processing operations
C) By limiting file sizes through saving all personal data that is processed in the smallest possible format
D) By limiting the personal data to what is adequate, relevant and necessary for the processing purposes

20 / 40
The GDPR refers to the principles of proportionality and subsidiarity.

What does **subsidiarity** mean?

A) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed.
B) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.
C) When processing personal data, a controller will only gather data which is necessary for the purpose.
D) When processing personal data, the means to be used shall be the least infringing upon privacy as possible.

21 / 40
What is the purpose of data lifecycle management (DLM)?

A) Assessing whether data should be treated as personal data or as normal data
B) Ensuring that personal data is deleted as soon as there is no lawful ground left to retain them
C) Managing the flow of data in a company in compliance with the GDPR

22 / 40
What is the **main** use of a persistent cookie?

A) To ensure that the user's personal data are stored securely on the server
B) To personalize the user's experience of the website during a next visit
C) To record every keystroke made by a computer user to find out passwords
D) To save the pages a user has bookmarked in the user's browser history

23 / 40
A cat rescue charity has many donors. They process personal data of these donors, both to keep records for tax purposes and for repeat donors. The donors have all consented to this processing.

The cat rescue wants to use an artificial intelligence (AI) system to automatically thank repeat donors by sending them cat videos of their favorite cats. The AI system will also e-mail one-time donors that more cats need help and suggest monthly donations.

Which GDPR principle is **especially** important for this AI system?

A) Accuracy, because the cat rescue must ensure that the AI system matches the cat videos to the donors well to get the best results and increase long-term donations.
B) Anonymization, because the cat rescue must ensure that the AI system does not have access to personal data in a form that makes donors recognizable.
C) Lawfulness, because the cat rescue is not a business which makes it more difficult to find a legitimate interest that the processing is necessary and lawful.
D) Transparency, because the cat rescue must inform the donors clearly on how their data is used and give a chance to object if they change the original purpose.

24 / 40
A company uses artificial intelligence (AI) to streamline its loan approval process. Loan applicants fill out an online form. The AI system analyzes this information and automatically decides if a person qualifies for a loan and how much they can borrow. This process is faster and more efficient than traditional methods, allowing the company to handle a larger number of applications quickly without needing human intervention.

According to the GDPR, what should this company do?

A) Anonymize the personal data that the AI uses to ensure that the loan applicants cannot be identified
B) Inform loan applicants about the automated decisions and offer them an easy way to request a human review
C) State clearly that the loan applicants must agree to the AI making automated decisions without human intervention
D) Stop using automated decisions and switch back to human decisions to ensure the loan applicants' rights

25 / 40
According to the GDPR, when are there **no** additional contracts needed for the transfer of personal data?

A) When both the sender and the recipient are in the European Economic Area (EEA)
B) When the sender encrypts the data before sending it to another company
C) When the data is not considered special category personal data
D) When the data is transferred for journalistic or artistic purposes

26 / 40
A company inside the European Economic Area (EAA) must draw up binding corporate rules (BCR).

According to the GDPR, what is a description of BCR?

A) A decision on the safety of transferring personal data to a non-EEA country
B) A measure to compensate for the lack of personal data protection in a third country
C) A set of agreements covering personal data transfers between non-EEA countries
D) A set of approved rules on personal data protection used by a group of enterprises

27 / 40
A controller wants to outsource processing of personal data to a processor.

What must **always** be done before outsourcing?

A) The controller and processor must draft and sign a written contract guaranteeing the confidentiality of the data.
B) The controller or processor must ask the supervisory authority for permission to outsource the processing of the data.
C) The controller must ask the supervisory authority if the agreed written contract is compliant with the regulations.
D) The processor must show the controller that all demands agreed in the service level agreement (SLA) are met.

28 / 40
A multinational company is planning to transfer personal data between its branches located in different countries, including those outside the European Economic Area (EEA). The company decides to implement binding corporate rules (BCR) to facilitate these transfers.

What is a necessary component of these BCR?

A) The BCR must guarantee financial compensation to data subjects in case of a personal data breach and specify the amount.
B) The BCR must include a mechanism for ensuring compliance with the rules by all employees involved in data processing.
C) The BCR must outline the specific organizational and technical measures used to protect personal data during transfers.
D) The BCR must specify that all data subjects should be notified of each personal data transfer in an accessible way.

29 / 40
A company wants to transfer personal data outside of the European Economic Area (EEA).

According to the GDPR, which transfers **outside** the EEA are always lawful?

A) Transfers based on the laws of the non-EEA country concerned
B) Transfers falling under World Trade Organization (WTO) rules
C) Transfers governed by approved binding corporate rules (BCR)
D) Transfers within a global corporation or organization

30 / 40
A company in France has binding corporate rules (BCR) for its worldwide operations. The company wants to transfer customer data to a third-party provider in the United States (U.S.), with which they are not in a joint operation.

The U.S. provider is not certified under the EU-U.S. Data Privacy Framework (DPF), but has signed standard contractual clauses (SCCs) that are approved by the European Commission (EC). These SCCs are part of a signed contract with the French company.

Under the GDPR, is this transfer of personal data to the U.S. provider lawful?

A) Yes, because the DPF has been declared invalid.
B) Yes, because the U.S. provider has signed SCCs.
C) No, because data transfers to the U.S. are forbidden.
D) No, because the U.S. provider should sign the BCR.

31 / 40
A coffee bar wants to use artificial intelligence (AI) and video surveillance to monitor how many cups of coffee the employees pour. Their goal is to understand which hours of the week are busiest, by monitoring the productivity.

According to the GDPR, is a data protection impact assessment (DPIA) **obligatory**?

A) Yes, because the processing is likely to result in a high risk to the rights of data subjects.
B) Yes, because the project includes AI technologies or processes that use personal data.
C) No, because no special category personal data are collected during the monitoring.
D) No, because the goal is not directly to assess the productivity of the employees.

32 / 40
During the data protection impact assessment (DPIA), a team working on a children's online platform explores whether using avatars instead of real names meets functionality needs.

Which DPIA objective is **most** supported by this action?

A) Assess necessity and proportionality
B) Describe the processing
C) Engage relevant stakeholders
D) Identify and assess risks to data subjects

33 / 40
The GDPR sets out the minimum features of a data protection impact assessment (DPIA).

What is one of these minimum features?

A) A detailed report on the data protection officer's (DPO) responsibilities and duties
B) A review of the organization's data sharing agreements with third parties
C) An evaluation of the security measures taken to protect data transfers
D) Measures to address the risks identified to the rights and freedoms of data subjects

34 / 40
While performing a backup, a data server disk crashed. Both the data and the backup are lost. The disk contained personal data from customers and other sensitive company data.

The processor states that this is a personal data breach according to the GDPR.

Is the statement of the processor true?

A) Yes, because the personal data on the server disk were unlawfully processed.
B) Yes, because the sensitive company data were also on the same server disk.
C) No, because the personal data on the disk were not processed, only destroyed.
D) No, because this is only a regular data breach and not a personal data breach.

35 / 40
A company is planning to process personal data. The recently appointed data protection officer (DPO) executes a data protection impact assessment (DPIA). The DPO finds that all computers have a setting causing monitors to show a screen saver after five seconds of inaction. However, the computers are not locked automatically. When employees leave their desk, they usually do not lock their computers either.

What is this an example of?

A) Data access
B) Personal data breach
C) Security incident
D) Security vulnerability

36 / 40
An architect leaves a building site. He puts his laptop down to answer his phone. A truck drives over the laptop. All his files on the design of the building and the calculations he worked on are lost. A back-up of an earlier version of the files is available in the cloud.

According to the GDPR, is this a personal data breach?

A) Yes, because destroying the last copy of a file makes them unavailable.
B) Yes, because the files destroyed were the architect's personal files.
C) No, because the design files and calculations are not personal data.
D) No, because the files are still available in the form of a back-up.

37 / 40
After a personal data breach, a controller within the European Economic Area (EEA) must determine who must be informed:

- No one
- Only the supervisory authority
- The supervisory authority and all data subjects affected

According to the GDPR, in what situation must **data subjects** be notified of a personal data breach?

A) When personal data is processed at a facility of the processor that is not located within the borders of the EEA
B) When personal data is processed by a party that agreed to the draft processing contract but has not yet signed it
C) When the system on which the personal data is processed is attacked, causing damage to its storage devices
D) When there is a significant probability that the breach will lead to a high risk for the privacy of the data subjects

38 / 40
A system containing personal data has been hacked and it was found that unauthorized persons have had access to the personal data.

According to the GDPR, what must the controller do **before** notifying the supervisory authority?

A) Assess whether personal data of a sensitive nature have or may have been accessed
B) Conduct a data protection impact assessment (DPIA) to assess the risk to natural persons
C) Notify the involved data subjects of the personal data breach and possible consequences
D) Notify the police and report the unauthorized access to the system or systems to them

39 / 40
Supervisory authorities have certain tasks aimed at ensuring compliance with the GDPR.

What is one of those tasks?

A) Assessing codes of conduct for specific sectors related to processing personal data
B) Defining a minimum set of measures to be taken to protect personal data and privacy
C) Drafting standard contractual clauses (SCC) and binding corporate rules (BCR)
D) Investigating all data breaches of which the supervisory authority has been notified

40 / 40
A controller has their headquarters within the European Economic Area (EEA). They have outsourced the processing of sensitive personal data to a processor outside the EEA, without consulting the supervisory authority first. This transgression was discovered, and the company was fined by the supervisory authority.

Six months later the supervisory authority learns that the controller is guilty of the same transgression, but for a different processing operation and with another processor.

What is the **maximum** fine the supervisory authority can impose in this case?

A) Nothing, because the company has already been fined for this transgression
B) Nothing, but a formal warning without financial penalties may be given
C) A fine of up to €10 M or 2% of turnover, whichever is higher
D) A fine of up to €20 M or 4% of turnover, whichever is higher

Answer key

1 / 40
What is the relationship between data protection and privacy?

A) Data protection and privacy are synonyms and have the same meaning.
B) Data protection is the part of privacy that protects a person's physical integrity.
C) Data protection refers to the measures needed to protect a person's privacy.

A) Incorrect. Data protection helps to protect a person's privacy, but the terms are not synonyms.
B) Incorrect. Data protection is not related to physical integrity or physical privacy.
C) Correct. Data protection are some of the measures needed to protect a person's privacy. (Literature: A, Chapter 1)

2 / 40
In the legal system of the European Union (EU), different tools are used to reach various goals. Some of these tools are binding, while others let EU Member States decide how to use them, offering them flexibility.

Does the GDPR allow this flexibility?

A) Yes, because it is a directive, which sets goals for EU Member States and sets out national measures.
B) Yes, because it is a recommendation that gives advice without further specific legal obligations.
C) No, because it is a decision that is binding only for specific parties and not for all EU Member States.
D) No, because it is a regulation, that applies to all EU Member States and is directly applicable.

A) Incorrect. A directive sets goals for the EU Member States, which then decide how to include them in their national law. However, the GDPR is a regulation.
B) Incorrect. A recommendation is non-binding and does not require any legal measures from the EU Member States. However, the GDPR is a regulation.
C) Incorrect. A decision is binding only on the specific parties it addresses, not on all EU Member States, and does not apply to everyone. However, the GDPR is a regulation.
D) Correct. The GDPR is a regulation which is fully binding and directly applicable across the EU, with no need for national measures. (Literature: A, Chapter 1)

3 / 40
How does the GDPR define personal data?

A) Any information relating to a resident of the European Economic Area (EEA)
B) Any information relating to an identified or identifiable natural person
C) Data that directly relate to an identified or identifiable natural person
D) Data that reveal someone's racial or ethnic background, religious views, health, sex life or sexual orientation

A) Incorrect. Information is only personal data if it relates to an identifiable or identified natural person. The place of residence is not relevant to determine whether data are personal data.
B) Correct. This is the official definition of the GDPR. (Literature: A, Chapter 1; GDPR Article 4(1))
C) Incorrect. Data are also personal data if they indirectly relate to an identifiable or identified natural person.
D) Incorrect. This is the definition of special personal data not of personal data.

4 / 40
According to the GDPR, what is the definition of processing of personal data?

A) Any operation that can be performed on personal data
B) Any operation that can be performed on personal data, except erasing and destroying
C) Only operations in which the personal data is shared or transferred in any way
D) Only operations in which the personal data is used for the purposes for which it was collected

A) Correct. Processing means any operation which is performed on personal data. (Literature: A, Chapter 1; GDPR Article 4(2))
B) Incorrect. Erasing and destroying are also processing of data.
C) Incorrect. Any operation, including distributing, falls under processing of data.
D) Incorrect. Any operation which is performed on personal data is regarded as processing.

5 / 40
The GDPR defines some personal data as special category data, sometimes called 'sensitive data'.

What is an example of this type of data?

A) A collection of employees' work email addresses
B) A genealogical register of someone's ancestors
C) A list of payments made using a credit card
D) An address list of members of a political party

A) Incorrect. Work email addresses are considered personal data but do not fall under special category personal data.
B) Incorrect. Genealogical information on living persons is personal data, but not special category personal data. The GDPR does not apply to data of deceased persons.
C) Incorrect. Credit card data is personal data, but not special category personal data.
D) Correct. Personal data revealing political opinions is special category personal data. (Literature: A, Chapter 4; GDPR Article 9(1))

6 / 40
One of the roles described in the GDPR is defined as:

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Which role is defined here?

A) Controller
B) Processor
C) Supervisory authority
D) Third party

A) Correct. The controller determines the purpose and means of the processing. (Literature: A, Chapter 2; GDPR Article 4(7))
B) Incorrect. The controller determines the purpose of the processing, the processor works on the controller's instructions.
C) Incorrect. The supervisory authority monitors and enforces compliance with the GDPR requirements.
D) Incorrect. A third party has no role in determining the purpose of the processing. Any party that determines the purpose would become a new controller.

7 / 40
Processing of personal data must be lawful. A company collects personal data of its customers.

What is **always** necessary for lawful processing when collecting personal data?

A) Asking permission from the supervisory authority for the processing
B) Documenting a legitimate ground for the processing of the personal data
C) Implementing a code of conduct describing the nature of the processing

A) Incorrect. Prior consultation is only obligatory when a data protection impact assessment (DPIA) indicates a high risk. (GDPR Article 36)
B) Correct. Processing is lawful only when a legitimate purpose exists. (Literature: A, Chapter 4; GDPR Article 6)
C) Incorrect. Codes of conduct may be a means to harmonize controller-processor contracts.

8 / 40
According to the GDPR, the controller must keep a record of all processing activities.

Which record is **not** obligatory according to the GDPR?

A) A record of all implemented technical and organizational measures of all processors
B) A record of all intended processing together with the processing purposes and legal justifications
C) A record of data breaches with all relevant characteristics, including notifications

A) Correct. Although the controller must verify that processors use appropriate technical and organizational measures, these measures do not need to be recorded. (Literature: A, Chapter 2; GDPR Article 28(1))
B) Incorrect. A record of all intended processing with the purpose(s) and legal justifications must be kept.
C) Incorrect. A record of data breaches must be kept.

9 / 40
One of the seven principles of data protection by design is *full functionality – positive-sum, not zero-sum*.

What is the essence of this principle?

A) Data protection coexists with security to create a win-win situation, which accomodates legitimate interests together with privacy.
B) Data protection includes informing data subjects about the ways their data is processed, which helps data subjects to stay in control.
C) Data protection is built into the architecture and design of the systems, which makes it a core functionality.

A) Correct. This is the essence of *full functionality – positive-sum, not zero-sum*. (Literature: A, Chapter 2)
B) Incorrect. This is the essence of *visibility and transparency - keep it open*.
C) Incorrect. This is the essence of *privacy embedded into design*.

10 / 40
What is a description of data protection by design and by default?

A) An approach that implements data protection from development
B) An indication of timeframes if processing relates to erasure
C) Data may only be collected for explicit and legitimate purposes
D) Not holding more data than is strictly required for processing

A) Correct. This is a correct description. (Literature: A, Chapter 2; GDPR Article 25)
B) Incorrect. This is a description of a data protection impact assessment (DPIA).
C) Incorrect. This is a description of measures taken to comply with the principle of purpose limitation.
D) Incorrect. This is a description of procedures to comply with the principle of data minimization.

11 / 40
To plan the amount of parking space needed, a local government monitors and saves the license plate number of every car that enters and leaves the city center. By comparing the license plate time of entry and exit the number of cars present every moment of each day is calculated.

They have obtained permission to collect data on the number of cars present in the city center. Each month a report is created detailing the average number of cars in the city center at specific moments for every day of the week.

At every entrance to the city center, a billboard clearly states what data is collected by whom, the purpose of the processing and the fact that the license plate numbers are saved securely for up to two years, because the measurements will be repeated next year.

Which of the basic principles for legitimate processing of personal data is **violated** in this scenario?

A) Personal data are collected for specified, explicit and legitimate purposes and not further processed.
B) Personal data are kept in a form permitting identification of data subjects for no longer than is necessary.
C) Personal data are processed in a manner that ensures appropriate security of the personal data.
D) Personal data are processed in a transparent manner in relation to the data subject.

A) Incorrect. The local government has specified their legitimate purpose to collect data on the number of cars present.
B) Correct. In the given scenario, there is no need to retain the data of a specific car identifying the owner once it has left the area. (Literature: A, Chapter 3; GDPR Article 5)
C) Incorrect. The scenario does not suggest inappropriate security.
D) Incorrect. The processing is taking place transparently, since it is communicated properly to the data subjects.

12 / 40
Further processing, after the original objective is fulfilled, is allowed in a few specific cases, provided that appropriate safeguards for the rights and freedoms of the data subjects are taken.

For which purpose is further processing **not** allowed?

A) For archiving purposes in the public interest
B) For direct marketing and commercial purposes
C) For generalized statistical purposes
D) For scientific or historical research purposes

A) Incorrect. With the safeguards in place, further processing is allowed for archiving purposes in the public interest.
B) Correct. This is not a purpose that is allowed, if it is not the original legitimate purpose of the processing. (Literature: A, Chapter 3)
C) Incorrect. With the safeguards in place, further processing is allowed for generalized statistical purposes.
D) Incorrect. With the safeguards in place, further processing is allowed for research purposes.

13 / 40
An organization provides its privacy notice in multiple languages and formats, including online, print, and audio, to ensure that all data subjects can access and understand it.

Which GDPR right does this practice support **most** directly?

A) The right to erasure, because data subjects are helped to understand that they have the right to delete their data any time.
B) The right to object, because data subjects can object to processing better when they understand the privacy notice completely.
C) The right to restriction, because data subjects are informed about the company's objectives and the legitimate grounds for processing.
D) The right to transparent information, communication, and modalities, because data subjects are helped to understand the privacy notice.

A) Incorrect. Although understanding their rights is important, the practice of providing privacy notices in various formats primarily supports transparency instead of directly facilitating the right to erasure.
B) Incorrect. Understanding privacy notices can help data subjects exercise their rights, but the main focus of this practice is enhancing transparency instead of directly supporting the right to object.
C) Incorrect. While informing data subjects about processing is necessary, the main purpose of providing accessible privacy notices is to ensure transparency, not specifically to support the right to restriction.
D) Correct. Providing privacy notices in multiple languages and formats ensures that all data subjects receive clear and accessible information, supporting their right to transparency. (Literature: A, Chapter 5)

14 / 40
Which data subject right is explicitly defined by the GDPR?

A) A copy of personal data must be provided in the format requested by the data subject.
B) Access to personal data must be provided free of charge for the data subject.
C) Personal data must always be changed at the request of the data subject.
D) Personal data must always be erased if the data subject requests this.

A) Incorrect. It must be provided in a structured, commonly used and machine-readable format, but not necessarily in any format the data subject specifies.
B) Correct. Data subjects have a right to a copy of their data free of charge. However, only the first copy has to be free. (Literature: A, Chapter 5)
C) Incorrect. Only erroneous data has to be rectified.
D) Incorrect. The right to erasure has several exceptions to this, for instance if the data are needed for the establishment, exercise or defense of legal claims.

15 / 40
A person buys a suit and provides the shop with his consent to use his e-mail address for advertising. Once the customer gets home, he asks the shop to erase all his personal data and stop sending him e-mails.

According to the GDPR, what must the shop do?

A) The shop may not delete any of his personal data since information about sales must be kept.
B) The shop must delete all personal data of this person for which the legitimate ground is consent.
C) The shop must delete his other personal data but can keep sending e-mails.

A) Incorrect. The shop has a legal obligation to retain data regarding the purchase. The data subject has withdrawn consent, hence only processing based on a legitimate ground other than consent can continue, and the shop must stop sending e-mails for advertising.
B) Correct. The shop has a legal obligation to retain data regarding the purchase (which are also personal data), but other data must be erased. The data subject has withdrawn consent, so the shop must stop sending e-mails for advertising. (Literature: A, Chapter 5; GDPR Article 17)
C) Incorrect. The data subject has withdrawn consent, so the shop must stop sending e-mails.

16 / 40
A person regularly receives offers from a store where he purchased something five years ago. He wants the company to stop sending offers and to delete his personal data.

Which of the data subjects' rights is he exercising?

A) The right of access
B) The right to object
C) The right to rectification
D) The right to restriction of processing

A) Incorrect. The right of access involves obtaining information about one's personal data and how it is processed, not stopping communications or requesting deletion.
B) Correct. The right to object allows the individual to request that the company stop processing his data for marketing purposes, which includes stopping the offers. (Literature: A, Chapter 5; GDPR Article 21)
C) Incorrect. The right to rectification is about correcting inaccurate or incomplete data, not stopping communications or erasing data.
D) Incorrect. Restriction is about blocking data that is incorrect or processed in contradiction with legal regulations.

17 / 40
A company uses artificial intelligence (AI) to analyze job application letters and automatically decide to invite them for an interview.

Which GDPR right is **most** relevant to this scenario?

A) The right not to be subject to a decision based solely on automated processing
B) The right to lodge a complaint with a supervisory authority
C) The right to restriction of processing
D) The right to transparent information, communication, and modalities

A) Correct. This right is most relevant, as it specifically addresses concerns about decisions made without human intervention, such as those made by AI in this scenario. (Literature: A, Chapter 5; GDPR Article 22)
B) Incorrect. Lodging a complaint is a general right for any GDPR violation, but it does not specifically relate to automated decision-making.
C) Incorrect. Restriction of processing involves limiting the use of personal data, not addressing decisions made by AI.
D) Incorrect. While transparency is important, it does not directly address the issue of automated decision-making in this scenario.

18 / 40
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Which data processing principle is described here?

A) Accuracy
B) Data minimization
C) Lawfulness, fairness, and transparency
D) Purpose limitation

A) Incorrect. Accuracy refers to ensuring the data is correct and up to date, not specifying the purposes for data collection.
B) Incorrect. Data minimization refers to collecting only the data necessary for a specific purpose, not specifying the purposes themselves.
C) Incorrect. Lawfulness, fairness, and transparency involve having a legal basis and being clear about processing, but do not specifically address purpose specification.
D) Correct. Purpose limitation requires that personal data be collected for specified, explicit, and legitimate purposes. (Literature: A, Chapter 3; GDPR Article 5)

19 / 40
The GDPR describes the principle of data minimization.

How can organizations comply with this principle?

A) By applying the concept of least privilege to the personal data collected, stored or otherwise processed
B) By limiting access rights to staff who need the personal data for the intended processing operations
C) By limiting file sizes through saving all personal data that is processed in the smallest possible format
D) By limiting the personal data to what is adequate, relevant and necessary for the processing purposes

A) Incorrect. Data minimization does not address least privilege, where users are given the fewest rights of access possible.
B) Incorrect. This describes the concept of limiting authorization for instance to comply with the principle of integrity and confidentiality.
C) Incorrect. Data minimization does not imply small storage size, but reducing the use of personal data to what is absolutely necessary.
D) Correct. This is the essence of the description of the data minimization principle in the GDPR. (Literature: A, Chapter 3; GDPR Article 5(1)(c))

20 / 40
The GDPR refers to the principles of proportionality and subsidiarity.

What does **subsidiarity** mean?

A) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed.
B) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.
C) When processing personal data, a controller will only gather data which is necessary for the purpose.
D) When processing personal data, the means to be used shall be the least infringing upon privacy as possible.

A) Incorrect. This is a definition of purpose limitation.
B) Incorrect. This is a definition of storage limitation.
C) Incorrect. This is a definition of data minimization.
D) Correct. If subsidiarity is applied to data protection, it means using the least intrusive ways to process data, minimizing impact on privacy. (Literature: A, Chapter 3; GDPR Recital 170)

21 / 40
What is the purpose of data lifecycle management (DLM)?

A) Assessing whether data should be treated as personal data or as normal data
B) Ensuring that personal data is deleted as soon as there is no lawful ground left to retain them
C) Managing the flow of data in a company in compliance with the GDPR

A) Incorrect. The purpose of DLM is to manage the flow of all data in a company and guarantee that data are processed securely and in compliance with the GDPR. It is not only about personal data, but about all data.
B) Incorrect. This is not the purpose of DLM. However, DLM helps to track data that should be deleted if there is no lawful ground to retain it.
C) Correct. DLM is a structured approach to manage the flow of data, determine necessary security controls and guarantee compliance with the GDPR. (Literature: A, Chapter 6; GDPR Article 5)

22 / 40
What is the **main** use of a persistent cookie?

A) To ensure that the user's personal data are stored securely on the server
B) To personalize the user's experience of the website during a next visit
C) To record every keystroke made by a computer user to find out passwords
D) To save the pages a user has bookmarked in the user's browser history

A) Incorrect. Cookies are not used to store data on the server.
B) Correct. This is the main purpose of a persistent cookie. (Literature: A, Chapter 7)
C) Incorrect. Cookies are not malicious by nature, but the mechanism can be exploited maliciously.
D) Incorrect. The bookmarks and browser history are saved, but not in a cookie.

23 / 40
A cat rescue charity has many donors. They process personal data of these donors, both to keep records for tax purposes and for repeat donors. The donors have all consented to this processing.

The cat rescue wants to use an artificial intelligence (AI) system to automatically thank repeat donors by sending them cat videos of their favorite cats. The AI system will also e-mail one-time donors that more cats need help and suggest monthly donations.

Which GDPR principle is **especially** important for this AI system?

A) Accuracy, because the cat rescue must ensure that the AI system matches the cat videos to the donors well to get the best results and increase long-term donations.
B) Anonymization, because the cat rescue must ensure that the AI system does not have access to personal data in a form that makes donors recognizable.
C) Lawfulness, because the cat rescue is not a business which makes it more difficult to find a legitimate interest that the processing is necessary and lawful.
D) Transparency, because the cat rescue must inform the donors clearly on how their data is used and give a chance to object if they change the original purpose.

A) Incorrect. In the context of the GDPR, accuracy refers to correctness of the data itself, not the of the algorithm. Accuracy, fairness, and bias are mandatory requirements in the AI Act.
B) Incorrect. The organization must use identifiable data to send personalized messages, so anonymization would not be relevant.
C) Incorrect. The cat rescue must have a lawful basis or a legitimate interest. However, finding one is not made more difficult by being a charity. Donors already consented to the processing of their personal data. The only thing missing is informing the donors and allowing them to object to additional processing.
D) Correct. Transparency is most important for this AI system, because using an AI system is a new processing activity. It is essential to update donors if the data processing purpose changes. (Literature: A, Chapter 3 and 7.2)

24 / 40
A company uses artificial intelligence (AI) to streamline its loan approval process. Loan applicants fill out an online form. The AI system analyzes this information and automatically decides if a person qualifies for a loan and how much they can borrow. This process is faster and more efficient than traditional methods, allowing the company to handle a larger number of applications quickly without needing human intervention.

According to the GDPR, what should this company do?

A) Anonymize the personal data that the AI uses to ensure that the loan applicants cannot be identified
B) Inform loan applicants about the automated decisions and offer them an easy way to request a human review
C) State clearly that the loan applicants must agree to the AI making automated decisions without human intervention
D) Stop using automated decisions and switch back to human decisions to ensure the loan applicants' rights

A) Incorrect. Anonymizing data will not allow the AI to do its work well. The GDPR does not require anonymization, but it does require the opportunity for a human review.
B) Correct. This option aligns with the GDPR by ensuring applicants are informed about AI decisions and can request a human review if they disagree with a decision. (Literature: A, Chapter 7.2)
C) Incorrect. Stating that applicants must agree to automated decisions does not fulfill GDPR requirements. The company must also offer options for human review.
D) Incorrect. The GDPR does not require companies to stop using AI for decisions. Instead, it emphasizes transparency and the possibility to request a human intervention.

25 / 40
According to the GDPR, when are there **no** additional contracts needed for the transfer of personal data?

A) When both the sender and the recipient are in the European Economic Area (EEA)
B) When the sender encrypts the data before sending it to another company
C) When the data is not considered special category personal data
D) When the data is transferred for journalistic or artistic purposes

A) Correct. No additional contracts are needed for data transfers within the EEA, since all member countries must adhere to the GDPR's data protection standards. (Literature: A, Chapter 8; GDPR Article 44)
B) Incorrect. While encryption is a good security practice, additional measures may still be needed if the data is transferred outside the EEA, depending on the destination country's data protection laws.
C) Incorrect. The need for additional measures does not solely depend on whether the data is special category; it also depends on the destination of the data transfer.
D) Incorrect. Even for journalistic or artistic purposes, personal data transfers outside the EEA require additional measures to ensure compliance with GDPR.

26 / 40
A company inside the European Economic Area (EAA) must draw up binding corporate rules (BCR).

According to the GDPR, what is a description of BCR?

A) A decision on the safety of transferring personal data to a non-EEA country
B) A measure to compensate for the lack of personal data protection in a third country
C) A set of agreements covering personal data transfers between non-EEA countries
D) A set of approved rules on personal data protection used by a group of enterprises

A) Incorrect. This refers to adequacy decisions.
B) Incorrect. This refers to appropriate safeguards.
C) Incorrect. The GDPR does not cover agreements between non-EEA countries.
D) Correct. BCR are a set of rules approved by the supervisory authorities. (Literature: A, Chapter 9; GDPR Article 47)

27 / 40
A controller wants to outsource processing of personal data to a processor.

What must **always** be done before outsourcing?

A) The controller and processor must draft and sign a written contract guaranteeing the confidentiality of the data.
B) The controller or processor must ask the supervisory authority for permission to outsource the processing of the data.
C) The controller must ask the supervisory authority if the agreed written contract is compliant with the regulations.
D) The processor must show the controller that all demands agreed in the service level agreement (SLA) are met.

A) Correct. There must be a written contract guaranteeing the confidentiality of the data, listing the purposes and means of processing as defined by the controller and specifying that the processor will only process on instruction of the controller. Both parties must sign this contract. (Literature: A, Chapter 2; GDPR Article 28(3))
B) Incorrect. The controller does not have to ask the supervisory authority for permission for each instance of outsourcing. The processor never has to ask permission.
C) Incorrect. The supervisory authority is not a legal counsel and will not check contracts for compliance.
D) Incorrect. An SLA is not enough as it will focus on operations, not necessarily on purposes.

28 / 40
A multinational company is planning to transfer personal data between its branches located in different countries, including those outside the European Economic Area (EEA). The company decides to implement binding corporate rules (BCR) to facilitate these transfers.

What is a necessary component of these BCR?

A) The BCR must guarantee financial compensation to data subjects in case of a personal data breach and specify the amount.
B) The BCR must include a mechanism for ensuring compliance with the rules by all employees involved in data processing.
C) The BCR must outline the specific organizational and technical measures used to protect personal data during transfers.
D) The BCR must specify that all data subjects should be notified of each personal data transfer in an accessible way.

A) Incorrect. BCR do not guarantee financial compensation in case of a personal data breach. They focus on compliance with data protection standards.
B) Correct. The BCR must include mechanisms for ensuring compliance by all employees, because the BCR must be binding and enforceable within the corporate group. (Literature: A, Chapter 9)
C) Incorrect. While BCR must ensure data protection, they do not need to specify the technologies used. BCR focus on compliance and enforceability.
D) Incorrect. BCR are internal rules for data transfer within a corporate group. Data subjects must know how their personal data is processed, but a notification of each transfer is unnecessary.

29 / 40
A company wants to transfer personal data outside of the European Economic Area (EEA).

According to the GDPR, which transfers **outside** the EEA are always lawful?

A) Transfers based on the laws of the non-EEA country concerned
B) Transfers falling under World Trade Organization (WTO) rules
C) Transfers governed by approved binding corporate rules (BCR)
D) Transfers within a global corporation or organization

A) Incorrect. This would also require an adequacy decision confirming that those laws are sufficient.
B) Incorrect. WTO only covers free trade of goods and services.
C) Correct. BCR approved by a supervisory authority involved make the transfer lawful. (Literature: A, Chapter 9; GDPR Article 47)
D) Incorrect. This would also require that they adopt official BCR.

30 / 40
A company in France has binding corporate rules (BCR) for its worldwide operations. The company wants to transfer customer data to a third-party provider in the United States (U.S.), with which they are not in a joint operation.

The U.S. provider is not certified under the EU-U.S. Data Privacy Framework (DPF), but has signed standard contractual clauses (SCCs) that are approved by the European Commission (EC). These SCCs are part of a signed contract with the French company.

Under the GDPR, is this transfer of personal data to the U.S. provider lawful?

A) Yes, because the DPF has been declared invalid.
B) Yes, because the U.S. provider has signed SCCs.
C) No, because data transfers to the U.S. are forbidden.
D) No, because the U.S. provider should sign the BCR.

A) Incorrect. The DPF is considered to be adequate. However, the validity of the DPF is not relevant here since the SCCs already provide an independent legal basis for the data transfer.
B) Correct. The use of SCCs approved by the EC is a valid legal mechanism for international data transfers under the GDPR, making the transfer lawful. (Literature: A, Chapter 9; GDPR Article 46(2)(c))
C) Incorrect. Data transfers to the U.S. are not categorically forbidden. They can be lawful if appropriate safeguards, such as SCCs or the DPF, are in place.
D) Incorrect. BCR are for intra-group data transfers and do not apply to third-party providers like the U.S. cloud provider. The SCCs serve as the appropriate mechanism for this transfer.

31 / 40
A coffee bar wants to use artificial intelligence (AI) and video surveillance to monitor how many cups of coffee the employees pour. Their goal is to understand which hours of the week are busiest, by monitoring the productivity.

According to the GDPR, is a data protection impact assessment (DPIA) **obligatory**?

A) Yes, because the processing is likely to result in a high risk to the rights of data subjects.
B) Yes, because the project includes AI technologies or processes that use personal data.
C) No, because no special category personal data are collected during the monitoring.
D) No, because the goal is not directly to assess the productivity of the employees.

A) Correct. Video surveillance can significantly impact the privacy and rights of employees, thus necessitating a DPIA to assess and mitigate potential high risks to their rights and freedoms. (Literature: A, Chapter 10; GDPR Article 35)
B) Incorrect. Although a DPIA is required, this is not because personal data are used or because AI is used. What makes the DPIA obligatory is the high risk of monitoring performance to the privacy and rights of the employees.
C) Incorrect. Even if no special category personal data are collected, a DPIA is still required if there is a high risk to people's rights, like with video surveillance.
D) Incorrect. The reason for collecting data does not change the need for a DPIA if there is a high risk to people's rights.

32 / 40
During the data protection impact assessment (DPIA), a team working on a children's online platform explores whether using avatars instead of real names meets functionality needs.

Which DPIA objective is **most** supported by this action?

A) Assess necessity and proportionality
B) Describe the processing
C) Engage relevant stakeholders
D) Identify and assess risks to data subjects

A) Correct. By exploring whether using avatars instead of real names meets functionality needs, the team is assessing whether the data processing is necessary and proportionate to achieving the platform's goals. (Literature: A, Chapter 10)
B) Incorrect. The avatar assessment does not describe the processing activities but instead evaluates alternatives to meet functionality needs.
C) Incorrect. The avatar assessment does not involve engaging stakeholders but instead evaluates if fewer of their personal data can be used to meet functionality needs.
D) Incorrect. The avatar assessment does not directly identify or assess risks. It is aimed at evaluating the necessity and proportionality of using personal data (real names) versus not needing them (avatars).

33 / 40
The GDPR sets out the minimum features of a data protection impact assessment (DPIA).

What is one of these minimum features?

A) A detailed report on the data protection officer's (DPO) responsibilities and duties
B) A review of the organization's data sharing agreements with third parties
C) An evaluation of the security measures taken to protect data transfers
D) Measures to address the risks identified to the rights and freedoms of data subjects

A) Incorrect. While the role of a DPO is important under the GDPR, the DPIA does not specifically require a report on their responsibilities and duties as one of its minimum features.
B) Incorrect. Although reviewing data sharing agreements is important for overall data protection compliance, it is not specifically listed as a minimum feature of a DPIA under the GDPR.
C) Incorrect. While evaluating security measures is part of ensuring data protection, a DPIA specifically focuses on assessing the risks to the rights and freedoms of data subjects and the measures to mitigate these risks, instead of just evaluating security measures for data transfers.
D) Correct. The GDPR sets out the minimum features of a DPIA: a description of the envisaged processing operations and the purposes of the processing; an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged to address the risks and demonstrate compliance with the GDPR. (Literature: A, Chapter 10; GDPR Article 35(7), Recital 84 and Recital 90)

34 / 40
While performing a backup, a data server disk crashed. Both the data and the backup are lost. The disk contained personal data from customers and other sensitive company data.

The processor states that this is a personal data breach according to the GDPR.

Is the statement of the processor true?

A) Yes, because the personal data on the server disk were unlawfully processed.
B) Yes, because the sensitive company data were also on the same server disk.
C) No, because the personal data on the disk were not processed, only destroyed.
D) No, because this is only a regular data breach and not a personal data breach.

A) Correct. Personal data irretrievably lost is regarded as 'a breach of security leading to unlawful destruction of personal data', which also makes it a personal data breach. (Literature: A, Chapter 11; GDPR Article 4(12))
B) Incorrect. The sensitive company data are not important to determine if there has been a personal data breach.
C) Incorrect. The GDPR sees accidental loss of personal data as unlawful processing , because it is not on instruction of the controller or processor. This makes it a personal data breach.
D) Incorrect. Losing company data would be a data loss, not a data breach. Losing personal data is removing access to the personal data which is considered a personal data breach (availability breach) under the GDPR.

35 / 40
A company is planning to process personal data. The recently appointed data protection officer (DPO) executes a data protection impact assessment (DPIA). The DPO finds that all computers have a setting causing monitors to show a screen saver after five seconds of inaction. However, the computers are not locked automatically. When employees leave their desk, they usually do not lock their computers either.

What is this an example of?

A) Data access
B) Personal data breach
C) Security incident
D) Security vulnerability

A) Incorrect. The data have not been accessed.
B) Incorrect. No personal data have been processed unauthorized yet, so it is not a breach.
C) Incorrect. Processing has yet to begin, there is no reason to assume an incident has taken place.
D) Correct. Confidentiality of the data cannot be guaranteed if employees leave their workstation without locking the computer. (Literature: A, Chapter 11; GDPR Article 5(1)(f))

36 / 40
An architect leaves a building site. He puts his laptop down to answer his phone. A truck drives over the laptop. All his files on the design of the building and the calculations he worked on are lost. A back-up of an earlier version of the files is available in the cloud.

According to the GDPR, is this a personal data breach?

A) Yes, because destroying the last copy of a file makes them unavailable.
B) Yes, because the files destroyed were the architect's personal files.
C) No, because the design files and calculations are not personal data.
D) No, because the files are still available in the form of a back-up.

A) Incorrect. No personal data were destroyed.
B) Incorrect. A personal file is not a synonym for personal data.
C) Correct. No personal data were destroyed, so this is not a personal data breach. (Literature: A, Chapter 11; GDPR Article 4(12))
D) Incorrect. There was no personal data breach, but not for this reason. No personal data were destroyed.

37 / 40
After a personal data breach, a controller within the European Economic Area (EEA) must determine who must be informed:

- No one
- Only the supervisory authority
- The supervisory authority and all data subjects affected

According to the GDPR, in what situation must **data subjects** be notified of a personal data breach?

A) When personal data is processed at a facility of the processor that is not located within the borders of the EEA
B) When personal data is processed by a party that agreed to the draft processing contract but has not yet signed it
C) When the system on which the personal data is processed is attacked, causing damage to its storage devices
D) When there is a significant probability that the breach will lead to a high risk for the privacy of the data subjects

A) Incorrect. The location where the data is processed is of no significance to the obligation to notify data subjects of personal data breaches.
B) Incorrect. Personal data processed by another party than the controller without a valid written contract is considered a personal data breach. In the given situation however, negative consequences for the data subjects are unlikely. Notifying the data subject is not obligatory in that case.
C) Incorrect. Damage to storage devices will make access to the data difficult or even impossible but does not imply illegal processing.
D) Correct. If there is a significant probability of negative impact on the data subjects, the controller is obliged to notify them of the breach. (Literature: A, Chapter 11)

38 / 40
A system containing personal data has been hacked and it was found that unauthorized persons have had access to the personal data.

According to the GDPR, what must the controller do **before** notifying the supervisory authority?

A) Assess whether personal data of a sensitive nature have or may have been accessed
B) Conduct a data protection impact assessment (DPIA) to assess the risk to natural persons
C) Notify the involved data subjects of the personal data breach and possible consequences
D) Notify the police and report the unauthorized access to the system or systems to them

A) Correct. According to GDPR Article 33(1), notice is not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons." The controller needs to ascertain that before reporting. (Literature: A, Chapter 11; GDPR Article 33(1))
B) Incorrect. A DPIA is performed before the actual processing to determine how the processing will be organized and which risks need to be mitigated.
C) Incorrect. Notification of the data subject is required only if the personal data breach may likely result in a high risk to the rights and freedoms of the data subjects.
D) Incorrect. Informing the police is not obligatory according to the GDPR. It may be wise.

39 / 40
Supervisory authorities have certain tasks aimed at ensuring compliance with the GDPR.

What is one of those tasks?

A) Assessing codes of conduct for specific sectors related to processing personal data
B) Defining a minimum set of measures to be taken to protect personal data and privacy
C) Drafting standard contractual clauses (SCC) and binding corporate rules (BCR)
D) Investigating all data breaches of which the supervisory authority has been notified

A) Correct. One of the responsibilities of supervisory authorities is to provide general advice on how to comply with the regulations. (Literature: A, Chapter 12)
B) Incorrect. A supervisory authority will give general advice on what is an appropriate level of security. They do not prescribe specific measures.
C) Incorrect. SCCs are created by the European Commission (EC). Supervisory authorities may approve BCR for data transfers, but companies draft them.
D) Incorrect. A supervisory authority does not have the obligation or capacity to investigate all personal data breaches of which they have been notified.

40 / 40
A controller has their headquarters within the European Economic Area (EEA). They have outsourced the processing of sensitive personal data to a processor outside the EEA, without consulting the supervisory authority first. This transgression was discovered, and the company was fined by the supervisory authority.

Six months later the supervisory authority learns that the controller is guilty of the same transgression, but for a different processing operation and with another processor.

What is the **maximum** fine the supervisory authority can impose in this case?

A) Nothing, because the company has already been fined for this transgression
B) Nothing, but a formal warning without financial penalties may be given
C) A fine of up to €10 M or 2% of turnover, whichever is higher
D) A fine of up to €20 M or 4% of turnover, whichever is higher

A) Incorrect. Each violation of the GDPR can be fined separately, especially if it involves different processing operations or processors, so previous fines do not exempt the company from new penalties.
B) Incorrect. Given that this is a repeated violation of GDPR rules, it is unlikely that only a warning would be issued, as fines are typically imposed for continued non-compliance.
C) Incorrect. Outsourcing processing of sensitive data without proper consultation is a serious breach, and repeated offenses can lead to higher fines under the GDPR.
D) Correct. This is the maximum fine for a repeated violation of this nature. The transfers of personal data to a recipient in a third country or an international organization are punishable under the highest fine. (Literature: A, Chapter 12; GDPR Article 33)

Evaluation

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

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

Contact EXIN

www.exin.com