Sample Exam

Edition 201912

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
A shopkeeper wants to register how many visitors enter his shop every day. A system detects the MAC-address of each visitor's smartphone. It is impossible for the shopkeeper to identify the owner of the phone from this signal, but telephone providers can link the MAC-address to the owner of the phone.

According to the GDPR, is the shopkeeper allowed to use this method?

A) Yes, because the shopkeeper cannot identify the owner of the telephone.
B) Yes, because the visitor has automatically consented by connecting to the Wi-Fi.
C) No, because the telephone's MAC-address must be regarded as personal data.
D) No, because the telephone providers are the owners of the MAC-addresses.

2 / 40
Personal data as defined in the GDPR can be divided into several types. One of these types is described:

Data that directly or indirectly reveal someone's racial or ethnic background, political, philosophical, religious views, union affiliation and data related to health or sex life and sexual orientation.

What type of personal data is this?

A) Direct personal data
B) Indirect personal data
C) Pseudonymized data
D) Special category personal data

3 / 40
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 in data protection is defined here?

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

4 / 40
A security breach has occurred in an information system that also holds personal data.

According to the GDPR, what is the very **first** thing the controller must do?

A) Ascertain whether the breach may have resulted in loss or unlawful processing of personal data
B) Assess the risk of adverse effects to the data subjects using a data protection impact assessment (DPIA)
C) Assess whether personal data of a sensitive nature has or may have been unlawfully processed
D) Report the breach immediately to all data subjects and the relevant supervisory authority

5 / 40
A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What is the **exact** term that is associated with this definition in the GDPR?

A) Confidentiality violation
B) Personal data breach
C) Security breach
D) Security incident

6 / 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.

7 / 40
When personal data are processed, who is ultimately responsible for demonstrating compliance with the GDPR?

A) Controller
B) Data protection officer (DPO)
C) Processor
D) Supervisory authority

8 / 40
According to the principle of purpose limitation, data should not be processed beyond the legitimate purpose defined. However, further processing 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

9 / 40
According to the GDPR, in what situation must data subjects **always** 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 sign 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

10 / 40
Some data processing falls outside of the material scope of the GDPR.

What type of processing is **not** subject to the GDPR?

A) Collecting name and address information for a gymnastics club
B) Creating a back-up of biometric data for data security purposes
C) Editing personal photographs before printing them at home

11 / 40
The GDPR does not define privacy as a term but uses the concept implicitly throughout the text.

What is a correct definition of privacy as implicitly used throughout the GDPR?

A) The fundamental right to protection of personal data, regardless of how it was obtained
B) The right not to be disturbed by uninvited people, nor being followed, spied on or monitored
C) The right to respect for one's private and family life, home and personal correspondence
D) The right to freedom of opinion and expression and to seeking, receiving and imparting information

12 / 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.

13 / 40
What is the legal status of the GDPR?

A) The GDPR is functional law in all member states of the EEA. Some Articles allow for member states law to provide for more specific rules.
B) The GDPR is a recommendation of the European Commission that EEA countries' law authorities improve their laws on the protection of personal data.
C) The GDPR sets out minimum conditions and requirements. Member states need to pass national laws to meet these minimum requirements.

14 / 40
In the GDPR, some types of personal data are regarded as special category personal data.

Which personal data are considered special category personal data?

A) A list of payments made using a credit card
B) An address list of members of a political party
C) A genealogical register of someone's ancestors

15 / 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. They have obtained permission to collect data on the number of cars present in 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. 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.

16 / 40
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Which data processing principle is described here?

A) Accuracy
B) Data minimization
C) Fairness and transparency
D) Purpose limitation

17 / 40
A person is moving from city A to city B, within an EEA member state. In city A he was a patient of the local hospital A. In city B, he becomes a patient of hospital B. The patient has opted out of the national electronic patients file system.

The patient asks hospital A to forward his medical file directly to hospital B.

According to the GDPR, what is allowed?

A) The hospital in A can send the data directly to hospital B, as requested by the patient
B) The hospital in A can send the file to hospital B, before the patient has requested it
C) The hospital in A can send the medical file to the data subject, but not to another hospital
D) The hospital in A cannot send the file, because there is no legitimate ground for processing

18 / 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

19 / 40
The GDPR refers to the principles of proportionality and subsidiarity.

What is the meaning of subsidiarity in this context?

A) Personal data can only be processed in accordance with the purpose specification.
B) Personal data cannot be reused without explicit and informed consent.
C) Personal data may only be processed when there are no other means to achieve the purposes.
D) Personal data must be adequate, relevant and not excessive in relation to the purposes.

20 / 40
"The controller shall implement appropriate technical and organizational measures for ensuring that (.) only personal data which are necessary for each specific purpose of the processing are processed."

Which term in the GDPR is defined here?

A) Compliance
B) Data protection by design and by default
C) Embedded data protection

21 / 40
While performing a backup, a data server disk crashed. Both the data and the backup are lost. The disk contained personal data, but no special category personal data.

The processor states that this is a personal data breach.

Is the statement of the processor true?

A) Yes, because the personal data on the disk were unlawfully processed.
B) Yes, because there were no special category personal data stored on the disk.
C) No, because no personal data on the disk were processed, only destroyed
D) No, because this is only a security incident and not a data breach

22 / 40
Organizations are obliged to keep a number of records to demonstrate compliance with the GDPR.

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

A) A record of all intended processing together with the processing purpose(s) and legal justifications
B) A record of data breaches with all relevant characteristics, including notifications
C) A record of notifications sent to the supervisory authority regarding processing of personal data
D) A record of processors including personal data provided and the period this data can be retained

23 / 40
A personal data breach has occurred, and the controller is writing a draft notification for the supervisory authority. The following information is already in the notification:

- The nature of the personal data breach and its possible consequences.
- Information regarding the parties that can provide additional information about the data breach.

What other information must the controller provide?

A) Information of local and national authorities that were informed about the data breach
B) Name and contact details of the data subjects whose data may have been breached
C) Suggested measures to mitigate the adverse consequences of the data breach
D) The information needed to access the personal data that have been breached

24 / 40
According to Article 33 of the GDPR the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify a personal data breach to the supervisory authority.

What is the maximum penalty for non-compliance with this notification obligation?

A) € 10.000.000 or 2% of the annual global turnover, whichever is higher
B) € 20.000.000 or 4% of the annual global turnover, whichever is higher
C) Up to € 500.000 with a minimum of € 120.000
D) Up to € 820.000 with a minimum of € 350.000

25 / 40
According to the GDPR, what is a task of a supervisory authority?

A) Implement technical and organizational measures to ensure compliance
B) Investigate security breaches of corporate information
C) Monitor and enforce the application of the GDPR

26 / 40
A Belgian company has their headquarters in France for tax purposes. They enter into a legally binding contract with a processor in the Netherlands for the processing of personal data of data subjects with various nationalities.

A personal data breach occurs. The supervisory authorities start an investigation.

Why is the French supervisory authority seen as the lead supervisory authority?

A) Because France is located in the middle of Europe
B) Because France is the largest of the three EEA countries
C) Because the company has their headquarters in France

27 / 40
On July 12, 2016 the European Commission implemented a ruling regarding the transfer of personal data between the EEA and the US. The ruling is based on the data protection measures described in the EU-US Privacy Shield.

What kind of a ruling is this?

A) Adequacy decision
B) Derogation
C) Legally binding contract
D) Treaty superseding the GDPR

28 / 40
A controller wants to outsource processing of personal data to a processor.

What must be done **before** outsourcing?

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

29 / 40
What is the purpose of a data protection audit by the supervisory authority?

A) To advise the controller on the mitigation of privacy risks to protect the controller from liability claims for non-compliance.
B) To fulfill the obligation in the GDPR to implement appropriate technical and organizational measures for data protection.
C) To monitor and enforce the application of the GDPR by assessing that processing is performed in compliance with the GDPR.

30 / 40
In order for personal data processing to be lawful, what is **always** a requirement?

A) A code of conduct must be in place, describing what the processing exactly entails.
B) The processing must be reported to and allowed by the supervisory authority.
C) There must be a legitimate ground for the processing of personal data.

31 / 40
Personal data can be transferred outside of the 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 rules
C) Transfers governed by approved binding corporate rules (BCR)
D) Transfers within a global corporation or organization

32 / 40
According to the GDPR, what is a description of binding corporate rules (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

33 / 40
A written contract between a controller and a processor is called a data processing agreement.

According to the GDPR, what does **not** have to be covered in the written contract?

A) The contractor code of business ethics and conduct that is used.
B) The information security and personal data breach procedures
C) The technical and organizational measures implemented
D) Which data are covered by the data processing agreement

34 / 40
One of the objectives of a data protection impact assessment (DPIA) is to strengthen the confidence of customers or citizens in the way personal data is processed and privacy is respected.

How can a DPIA strengthen the confidence?

A) The organization minimizes the risk of costly adjustments in processes or the redesign of systems in a later stage
B) The organization prevents non-compliance with the GDPR and minimizes the risk of fines
C) The organization proves that it takes privacy seriously and aims for compliance with the GDPR

35 / 40
One of the seven principles of data protection by design is *Functionality – Positive-Sum, not Zero-Sum*.

What is the essence of this principle?

A) Applied security standards must assure the confidentiality, integrity and availability of personal data throughout their lifecycle.
B) If different types of legitimate objectives are contradictory, the privacy objectives must be given priority over other security objectives.
C) When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired.
D) Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks.

36 / 40
A company wishes to use personal data of their customers. They wish to start sending all female customers a customized newsletter.

What right do all data subjects have in this scenario?

A) The right to compensation
B) The right to object to profiling
C) The right to rectification

37 / 40
What is a description of data protection by design and by default?

A) An approach that implements data protection from the start
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

38 / 40
According to the GDPR, when is a data protection impact assessment (DPIA) obligatory?

A) When a project includes technologies or processes that use personal data
B) When processing is likely to result in a high risk to the rights of data subjects
C) When similar processing operations with comparable risks are repeated

39 / 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

40 / 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

Answer Key

1 / 40
A shopkeeper wants to register how many visitors enter his shop every day. A system detects the MAC-address of each visitor's smartphone. It is impossible for the shopkeeper to identify the owner of the phone from this signal, but telephone providers can link the MAC-address to the owner of the phone.

According to the GDPR, is the shopkeeper allowed to use this method?

A) Yes, because the shopkeeper cannot identify the owner of the telephone.
B) Yes, because the visitor has automatically consented by connecting to the Wi-Fi.
C) No, because the telephone's MAC-address must be regarded as personal data.
D) No, because the telephone providers are the owners of the MAC-addresses.

A) Incorrect. The issue is not whether the shopkeeper can identify the visitor, but that it is technically possible to do so.
B) Incorrect. Consent must be an active, informed and free act of agreement to the processing. To see a MAC-address, the visitor does not need to be logged onto the Wi-Fi.
C) Correct. The phone's signal is a unique code that can be linked to the owner of the phone. The data must be regarded as personal data, because it is technically possible to identify the visitor. (Literature: A, Chapter 3; GDPR Article 26 and 30)
D) Incorrect. The shopkeeper is not allowed to keep the data or process it because it must be regarded as personal data. The telephone provider is not the owner of the MAC-address, nor is the telephone provider protected by the GDPR.

2 / 40
Personal data as defined in the GDPR can be divided into several types. One of these types is described:

Data that directly or indirectly reveal someone's racial or ethnic background, political, philosophical, religious views, union affiliation and data related to health or sex life and sexual orientation.

What type of personal data is this?

A) Direct personal data
B) Indirect personal data
C) Pseudonymized data
D) Special category personal data

A) Incorrect. Both direct and indirect data are described.
B) Incorrect. Both direct and indirect data are described.
C) Incorrect. Pseudonymized data cannot directly reveal information.
D) Correct. This is a definition of special category personal data. (Literature: A, Chapter 1; GDPR Article 4).

3 / 40

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 in data protection 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 1; 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.

4 / 40

A security breach has occurred in an information system that also holds personal data.

According to the GDPR, what is the very **first** thing the controller must do?

A) Ascertain whether the breach may have resulted in loss or unlawful processing of personal data
B) Assess the risk of adverse effects to the data subjects using a data protection impact assessment (DPIA)
C) Assess whether personal data of a sensitive nature has or may have been unlawfully processed
D) Report the breach immediately to all data subjects and the relevant supervisory authority

A) Correct. The very first thing that needs to be done is ascertain that the security incident is in fact a personal data breach. (Literature: A, Chapter 5)
B) Incorrect. A DPIA is conducted when designing personal data processing operations. It is not a part of the procedure for a data breach.
C) Incorrect. This is the next step if the incident proves to be a personal data breach – ascertain what type of data breach.
D) Incorrect. Whether the data breach needs to be reported and to whom depends on whether it is a data breach and if so, the type of data breach.

5 / 40

A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What is the **exact** term that is associated with this definition in the GDPR?

A) Confidentiality violation
B) Personal data breach
C) Security breach
D) Security incident

A) Incorrect. GDPR uses the term personal data breach. Not every data breach is a confidentiality violation.
B) Correct. This is the definition of a personal data breach. (Literature: A, Chapter 5; GDPR Article 4(12))
C) Incorrect. GDPR uses the term personal data breach. Not every security breach is a data breach. Not every data breach is a personal data breach.
D) Incorrect. GDPR uses the term personal data breach. Not every security incident is a data breach.

6 / 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 4)
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.

7 / 40
When personal data are processed, who is ultimately responsible for demonstrating compliance with the GDPR?

A) Controller
B) Data protection officer (DPO)
C) Processor
D) Supervisory authority

A) Correct. The controller is responsible for adequate data security measures and must be able to demonstrate compliance with the GDPR. (Literature: A, Chapter 2)
B) Incorrect. The DPO has expert knowledge and assists the controller or processor to monitor internal compliance.
C) Incorrect. The processor is the one who processes personal data according to the instructions of the controller. The controller remains ultimately responsible though.
D) Incorrect. The controller needs to demonstrate compliance with the GDPR if requested by the supervisory authority.

8 / 40
According to the principle of purpose limitation, data should not be processed beyond the legitimate purpose defined. However, further processing 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 2)
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.

9 / 40
According to the GDPR, in what situation must data subjects **always** 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 sign 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 5)

10 / 40
Some data processing falls outside of the material scope of the GDPR.

What type of processing is **not** subject to the GDPR?

A) Collecting name and address information for a gymnastics club
B) Creating a back-up of biometric data for data security purposes
C) Editing personal photographs before printing them at home

A) Incorrect. Collecting is also considered processing data.
B) Incorrect. Storage is also considered processing data.
C) Correct. The GDPR is not applicable to home-use of your own photographs. (Literature: A, Chapter 1; GDPR Article 4)

11 / 40
The GDPR does not define privacy as a term but uses the concept implicitly throughout the text.

What is a correct definition of privacy as implicitly used throughout the GDPR?

A) The fundamental right to protection of personal data, regardless of how it was obtained
B) The right not to be disturbed by uninvited people, nor being followed, spied on or monitored
C) The right to respect for one's private and family life, home and personal correspondence
D) The right to freedom of opinion and expression and to seeking, receiving and imparting information

A) Incorrect. This is a definition of data protection.
B) Incorrect. This is a definition of physical privacy. However, the GDPR does not concern itself with physical privacy.
C) Correct. This is the definition as implicitly used throughout the GDPR. (Literature: A, Chapter 1)
D) Incorrect. This is a short version of Universal Declaration of Human Rights Article 19: freedom of opinion and expression.

12 / 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)

13 / 40
What is the legal status of the GDPR?

A) The GDPR is functional law in all member states of the EEA. Some Articles allow for member states law to provide for more specific rules.
B) The GDPR is a recommendation of the European Commission that EEA countries' law authorities improve their laws on the protection of personal data.
C) The GDPR sets out minimum conditions and requirements. Member states need to pass national laws to meet these minimum requirements.

A) Correct. The GDPR is European law but the Regulation does not exclude Member state law that sets out the circumstances for specific processing situations. (Literature: A, Chapter 1; GDPR Recital 10)
B) Incorrect. An EU recommendation is not binding. The GDPR is functional European law in all member states.
C) Incorrect. This is the description of an EU Directive.

14 / 40
In the GDPR, some types of personal data are regarded as special category personal data.

Which personal data are considered special category personal data?

A) A list of payments made using a credit card
B) An address list of members of a political party
C) A genealogical register of someone's ancestors

A) Incorrect. Credit card data is personal data, but not special category data.
B) Correct. Personal data revealing political opinions is special personal data (Literature: A, Chapter 1; GDPR Article 9(1))
C) Incorrect. Genealogical information on living persons is personal data, but not special category. The GDPR does not apply to data on deceased persons.

15 / 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. They have obtained permission to collect data on the number of cars present in 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. 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 is entitled 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 2; 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.

16 / 40
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Which data processing principle is described here?

A) Accuracy
B) Data minimization
C) Fairness and transparency
D) Purpose limitation

A) Incorrect. Accuracy is the principle that personal data shall be accurate and kept up to date.
B) Correct. Data minimization means that personal data shall be adequate, relevant and limited to what is necessary. (Literature: A, Chapter 2; GDPR Article 5(1))
C) Incorrect. Fairness and transparency mean that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
D) Incorrect. Purpose limitation means that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with GDPR Article 89(1), not be considered to be incompatible with the initial purposes.

17 / 40
A person is moving from city A to city B, within an EEA member state. In city A he was a patient of the local hospital A. In city B, he becomes a patient of hospital B. The patient has opted out of the national electronic patients file system.

The patient asks hospital A to forward his medical file directly to hospital B.

According to the GDPR, what is allowed?

A) The hospital in A can send the data directly to hospital B, as requested by the patient
B) The hospital in A can send the file to hospital B, before the patient has requested it
C) The hospital in A can send the medical file to the data subject, but not to another hospital
D) The hospital in A cannot send the file, because there is no legitimate ground for processing

A) Correct. The right to portability allows this. (Literature: A, Chapter 3)
B) Incorrect. The hospital in B can only acquire the file from A with consent or if it is in the vital interest of the data subject and consent cannot be obtained.
C) Incorrect. The data subject can ask for the data to be sent directly.
D) Incorrect. A request, which implies consent, of the data subject is a sufficient legitimate ground.

18 / 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 has 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 2; GDPR Article 5(1)(f))

19 / 40
The GDPR refers to the principles of proportionality and subsidiarity.

What is the meaning of subsidiarity in this context?

A) Personal data can only be processed in accordance with the purpose specification.
B) Personal data cannot be reused without explicit and informed consent.
C) Personal data may only be processed when there are no other means to achieve the purposes.
D) Personal data must be adequate, relevant and not excessive in relation to the purposes.

A) Incorrect. This is one of the legal limitations.
B) Incorrect. This is one of the legal limitations.
C) Correct. This is the definition of subsidiarity. (Literature: A, Chapter 3; GDPR Article 35(7))
D) Incorrect. This is the definition of proportionality.

20 / 40
"The controller shall implement appropriate technical and organizational measures for ensuring that (.) only personal data which are necessary for each specific purpose of the processing are processed."

Which term in the GDPR is defined here?

A) Compliance
B) Data protection by design and by default
C) Embedded data protection

A) Incorrect. Compliance means meeting rules or standards.
B) Correct. By default, the minimum of personal data is to be processed for the shortest possible period, using the best possible security measures to prevent unauthorized access. Data protection by design refers to processing that includes appropriate measures to implement data protection principles. (Literature: A, Chapter 8; GDPR Article 25)
C) Incorrect. Embedded data protection is the result of data protection by design.

21 / 40
While performing a backup, a data server disk crashed. Both the data and the backup are lost. The disk contained personal data, but no special category personal data.

The processor states that this is a personal data breach.

Is the statement of the processor true?

A) Yes, because the personal data on the disk were unlawfully processed.
B) Yes, because there were no special category personal data stored on the disk.
C) No, because no personal data on the disk were processed, only destroyed
D) No, because this is only a security incident and not a 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 5; GDPR Article 4(12))
B) Incorrect. Accidental loss of data is a security incident (data is no longer available). According to the GDPR it is also unlawful processing of personal data, hence a personal data breach. Data do not have to belong to the category of special personal data to fall under the category personal data breach.
C) Incorrect. A technical malfunction causing data to be no longer available is a security incident. The GDPR sees accidental loss of personal data as unlawful processing (not on instruction of the controller or processor) hence as a personal data breach.
D) Incorrect. Personal data that are irretrievably lost, is regarded as unauthorized processing by the GDPR, hence a personal data breach. The fact that data was accidentally destroyed also makes the event a security incident.

22 / 40
Organizations are obliged to keep a number of records to demonstrate compliance with the GDPR.

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

A) A record of all intended processing together with the processing purpose(s) and legal justifications
B) A record of data breaches with all relevant characteristics, including notifications
C) A record of notifications sent to the supervisory authority regarding processing of personal data
D) A record of processors including personal data provided and the period this data can be retained

A) Incorrect. A record of all intended processing with the purpose(s) and legal justifications must be kept..
B) Incorrect. A record of data breaches must be kept.
C) Correct. Prior consultation of high-risk processing is obligatory, but there is no need for a separate record of notifications sent. (Literature: A, Chapter 6; GDPR Article 36(1))
D) Incorrect. A record of processors and data provided must be kept.

23 / 40
A personal data breach has occurred, and the controller is writing a draft notification for the supervisory authority. The following information is already in the notification:

- The nature of the personal data breach and its possible consequences.
- Information regarding the parties that can provide additional information about the data breach.

What other information must the controller provide?

A) Information of local and national authorities that were informed about the data breach
B) Name and contact details of the data subjects whose data may have been breached
C) Suggested measures to mitigate the adverse consequences of the data breach
D) The information needed to access the personal data that have been breached

A) Incorrect. The supervisory authority must be made aware of reports to supervisory authorities in other EEA countries. Reports to local authorities, for instance the police, do not need to be reported.
B) Incorrect. The supervisory authority requires an estimate of the number of data subjects involved, not their personal data.
C) Correct. The controller should add suggested measures to mitigate the adverse consequences of the data breach. (Literature: A, Chapter 7; GDPR Article 33(d))
D) Incorrect. The supervisory authority needs to know the type of personal data involved, but does not need access to the data themselves.

24 / 40
According to Article 33 of the GDPR the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify a personal data breach to the supervisory authority.

What is the maximum penalty for non-compliance with this notification obligation?

A) € 10.000.000 or 2% of the annual global turnover, whichever is higher
B) € 20.000.000 or 4% of the annual global turnover, whichever is higher
C) Up to € 500.000 with a minimum of € 120.000
D) Up to € 820.000 with a minimum of € 350.000

A) Correct. This is the maximum according to the GDPR for infringement of the personal data breach notification obligation. (Literature: A, Chapter 7; GDPR Article 33)
B) Incorrect. This fine is given for non-compliance or non-conformity to the basic principles for processing, including conditions for consent.
C) Incorrect. This is an outdated number based on the Dutch Penal code. GDPR rules specify higher fines.
D) Incorrect. This is an outdated number based on the Dutch Penal code. GDPR rules specify higher fines.

25 / 40
According to the GDPR, what is a task of a supervisory authority?

A) Implement technical and organizational measures to ensure compliance
B) Investigate security breaches of corporate information
C) Monitor and enforce the application of the GDPR

A) Incorrect. This is the task of the controller.
B) Incorrect. Only breaches of personal data are a concern of the supervisory authority.
C) Correct. This is the main task of any supervisory authority. (Literature: A, Chapter 7)

26 / 40
A Belgian company has their headquarters in France for tax purposes. They enter into a legally binding contract with a processor in the Netherlands for the processing of personal data of data subjects with various nationalities.

A personal data breach occurs. The supervisory authorities start an investigation.

Why is the French supervisory authority seen as the lead supervisory authority?

A) Because France is located in the middle of Europe
B) Because France is the largest of the three EEA countries
C) Because the company has their headquarters in France

A) Incorrect. The geographical position of the countries is irrelevant.
B) Incorrect. The size of the countries is irrelevant.
C) Correct. The country of the main establishment determines the lead supervisory authority. The 'main establishment' is the place of the central administration of that organization, or in other words: headquarters. (Literature: A, Chapter 7)

27 / 40
On July 12, 2016 the European Commission implemented a ruling regarding the transfer of personal data between the EEA and the US. The ruling is based on the data protection measures described in the EU-US Privacy Shield.

What kind of a ruling is this?

A) Adequacy decision
B) Derogation
C) Legally binding contract
D) Treaty superseding the GDPR

A) Correct. The ruling is an adequacy decision regarding processing in third countries. (Literature: A, Chapter 7; GDPR Article 45 and Recitals (104) and (106))
B) Incorrect. A derogation is for specific situations where a transfer is necessary, but there is no ruling permitting it. (Literature: GDPR Article 49(1)(d))
C) Incorrect. The ruling is an adequacy decision. A legally binding contract is between a processor and a controller.
D) Incorrect. The ruling is an adequacy decision. It does not supersede the GDPR.

28 / 40
A controller wants to outsource processing of personal data to a processor.

What must be done **before** outsourcing?

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

A) Incorrect. The controller does not have to ask the supervisory authority for permission for each instance of outsourcing.
B) Incorrect. The supervisory authority is not a legal counsel and will not check contracts for compliance.
C) 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 processor will only process on instruction of the controller. Both parties must sign this contract. (Literature: A, Chapter 8; GDPR Article 28(3))
D) Incorrect. An SLA is not enough as it will focus on operations, not necessarily on purposes.

29 / 40
What is the purpose of a data protection audit by the supervisory authority?

A) To advise the controller on the mitigation of privacy risks to protect the controller from liability claims for non-compliance.
B) To fulfill the obligation in the GDPR to implement appropriate technical and organizational measures for data protection.
C) To monitor and enforce the application of the GDPR by assessing that processing is performed in compliance with the GDPR.

A) Incorrect. The supervisory authority has the task to monitor compliance and to advise on enhancements, but its purpose is not to protect the controller.
B) Incorrect. The audit is not the implementation of the measures, but an assessment of the effectiveness of them.
C) Correct. According to the GDPR this is an important task of a supervisory authority. (Literature: A, Chapter 7; GDPR Article 57 (1)(a))

30 / 40
In order for personal data processing to be lawful, what is **always** a requirement?

A) A code of conduct must be in place, describing what the processing exactly entails.
B) The processing must be reported to and allowed by the supervisory authority.
C) There must be a legitimate ground for the processing of personal data.

A) Incorrect. Codes of conduct may be a means to harmonize controller-processor contracts.
B) Incorrect. Prior consultation is only obligatory when a DPIA indicates a high risk. (GDPR Article 36)
C) Correct. Processing is lawful only when a legitimate purpose exists. (Literature: A, Chapter 3; GDPR Article 6)

31 / 40
Personal data can be transferred outside of the 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 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. Binding corporate rules approved by a supervisory authority involved make the transfer lawful. (Literature: A, Chapter 7; GDPR Article 47)
D) Incorrect. This would also require that they adopt official binding corporate rules.

32 / 40
According to the GDPR, what is a description of binding corporate rules (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 3; GDPR Article 47)

33 / 40
A written contract between a controller and a processor is called a data processing agreement.

According to the GDPR, what does **not** have to be covered in the written contract?

A) The contractor code of business ethics and conduct that is used.
B) The information security and personal data breach procedures
C) The technical and organizational measures implemented
D) Which data are covered by the data processing agreement

A) Correct. Although the GDPR endorses the use of codes of conduct and certification, it is not an obligation to have this clause to demonstrate compliance with the GDPR. (Literature: A, Chapter 8; GDPR Article 28(3))
B) Incorrect. This is mandatory because it describes the obligations of the processor regarding the notification of a personal data breach (by the controller) to the supervisory authority.
C) Incorrect. This is mandatory because it describes technical and organizational measures the processor must take.
D) Incorrect. This is mandatory because it describes the personal data, including special category personal data, covered by the contract.

34 / 40
One of the objectives of a data protection impact assessment (DPIA) is to strengthen the confidence of customers or citizens in the way personal data is processed and privacy is respected.

How can a DPIA strengthen the confidence?

A) The organization minimizes the risk of costly adjustments in processes or the redesign of systems in a later stage
B) The organization prevents non-compliance with the GDPR and minimizes the risk of fines
C) The organization proves that it takes privacy seriously and aims for compliance with the GDPR

A) Incorrect. This aspect may strengthen the confidence of management, but not of customers or citizens.
B) Incorrect. Preventing fines may strengthen the confidence of management, but not of customers or citizens.
C) Correct. Doing a DPIA shows customers or citizens that the company is serious about data protection. (Literature: A, Chapter 8)

35 / 40
One of the seven principles of data protection by design is *Functionality – Positive-Sum, not Zero-Sum*.

What is the essence of this principle?

A) Applied security standards must assure the confidentiality, integrity and availability of personal data throughout their lifecycle.
B) If different types of legitimate objectives are contradictory, the privacy objectives must be given priority over other security objectives.
C) When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired.
D) Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks.

A) Incorrect. This is an aspect of End-to-End Security – Lifecycle Protection, one of the other six basic principles
B) Incorrect. Data protection by design rejects the idea that privacy competes with other interests, design objectives, and technical capabilities.
C) Correct. This is the essence. (Literature: A, Chapter 8; GDPR Article 25)
D) Incorrect. This is an aspect of Privacy Embedded into Design, one of the other six basic principles

36 / 40
A company wishes to use personal data of their customers. They wish to start sending all female customers a customized newsletter.

What right do all data subjects have in this scenario?

A) The right to compensation
B) The right to object to profiling
C) The right to rectification

A) Incorrect. It is unlikely that all data subjects will suffer harm that must be compensated in this scenario.
B) Correct. All data subjects have a right to object to the processing of personal data for direct marketing, including profiling. This is clearly profiling. (Literature: A, Chapter 4)
C) Incorrect. It is unlikely that the company has incorrect data on all data subjects, so the right to rectification does not apply.

37 / 40
What is a description of data protection by design and by default?

A) An approach that implements data protection from the start
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 8; GDPR Article 25(1))
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.

38 / 40
According to the GDPR, when is a data protection impact assessment (DPIA) obligatory?

A) When a project includes technologies or processes that use personal data
B) When processing is likely to result in a high risk to the rights of data subjects
C) When similar processing operations with comparable risks are repeated

A) Incorrect. Only for technologies and processes that are likely to result in a high risk to the rights of data subjects is the DPIA mandatory.
B) Correct. For processing operations which are likely to result in a high risk, a DPIA is obligatory to assess those risks and to design mitigation measures. (Literature: A, Chapter 6; GDPR Article 35)
C) Incorrect. This is a case in which a DPIA does not need to be repeated.

39 / 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.
B) Incorrect. This describes the concept of limiting authorization for instance to comply with the principle of integrity and confidentiality
C) Incorrect. Data minimization according to the GDPR is not about storage size, but about minimalizing the use of personal data.
D) Correct. This is the essence of the description in the GDPR. (Literature: A, Chapter 2; GDPR Article 5(1)(c))

40 / 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 8)
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.

Evaluation

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

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

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER