Sample Exam

Edition 201803

Content

Introduction

This is the sample exam EXIN Privacy & Data Protection Foundation (PDPF.EN). 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 the correct answer.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth one point. If you obtain 26 points or more you will pass.

The time allowed for this exam is 60 minutes.

Good luck!

Sample Exam

1 / 40
The illegal collection, storage, modification, disclosure or dissemination of personal data is an offence by European law.

What kind of offence is this?

A) a content related offence
B) an economic offence
C) an intellectual property offence
D) a privacy offence

2 / 40
How are privacy and data protection related to each other?

A) Data protection is a subset of privacy.
B) Privacy is a subset of data protection.
C) They are the same thing.
D) You cannot have privacy without data protection.

3 / 40
What is the GDPR **mainly** intended for?

A) To be a common ground upon which the member states can build their own laws.
B) To make non-EU countries respect the right to privacy of individuals within the EU.
C) To secure privacy as a fundamental human right for everyone.
D) To strengthen and unify data protection for individuals within the EU.

4 / 40
The GDPR is related to personal data protection.

What is the definition of personal data?

A) any information relating to an identified or identifiable natural person
B) any information that the European citizens would like to protect
C) data that directly or indirectly reveal someone's racial or ethnic background, religious views, and data related to health or sexual habits
D) preservation of confidentiality, integrity and availability of information

5 / 40
According to the GDPR, which personal data category is regarded as sensitive data?

A) credit card details
B) trade union membership
C) passport number
D) social security number

6 / 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 data is being shared on social media or transferred by email or otherwise through the Internet
D) Only operations in which the personal data is used for the purposes for which it was collected

7 / 40
"An independent public authority which is established by a Member State pursuant to Article 51."

Which role in data protection is defined?

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

8 / 40
'Informed consent' is a lawful basis to process personal data under the GDPR. The purpose of the processing for which consent is given should be documented.

At what time in the process should the data subject's consent be obtained?

A) After the purpose specification is presented and before personal data is collected.
B) Before the purpose specification is conceived and presented.
C) Before the personal data is processed.
D) Before the personal data is published or disseminated.

9 / 40
The GDPR is based on the principles of proportionality and subsidiarity.

What is the meaning of 'proportionality' in this context?

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

10 / 40
The processing of personal data has to meet certain quality requirements.

What is one of these quality requirements defined by the GDPR?

A) The data processed must be archived.
B) The data processed must be encrypted.
C) The data processed must be indexed.
D) The data processed must be relevant.

11 / 40
Every time personal data is processed proportionality and subsidiarity must be checked.

What is the requirement for the personal data being processed?

A) It must be limited always to what is necessary to achieve the defined goals and must be limited to the least “intrusive” data.
B) It must be handled by the smallest number of employees possible and they must work for the Controller or an affiliate.
C) It must be limited to a predefined storage size and the system used must be financed by the Controller.
D) It must be used for the smallest number of purposes possible and this may not be done outside the premises of the Processor.

12 / 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?

A) Compliance
B) Data protection by default
C) Privacy by design
D) Embedded protection

13 / 40
What is the term used in the GDPR for unauthorized disclosure of, or access to, personal data?

A) Confidentiality violation
B) Data breach
C) Incident
D) Security incident

14 / 40
It has been ascertained that a data breach of sensitive personal data occurred.

To whom must this ultimately be reported according to the GDPR?

A) the supervisory authority
B) the Data Protection Officer (DPO)
C) the manager of the department
D) the police

15 / 40
While performing a backup, a data server disk crashes. Both the data and the backup are lost. The disk contained personal data but no sensitive data.

What kind of incident is this?

A) data breach
B) security breach
C) security incident

16 / 40
Someone working for a trade union took a draft newsletter for the members home to finish it there. The USB stick containing the draft and the mailing list, was lost.

To whom, among others, should this data breach be reported?

A) all members on the mailing list
B) the board of the trade union
C) the police

17 / 40
A social services organization plans to design a new database to administrate its clients and the care they need.

In order to request permission with the supervisory authority, what is one of the first important steps to be taken?

A) Collect data about the clients and the amount and kind of care needed and provided.
B) Conduct a data protection impact assessment (DPIA) to assess the risks of the intended processing.
C) Obtain consent of the clients for the intended processing of their personal data.

18 / 40
In which case should the data subjects always be notified of a data breach?

A) The personal data was processed at a facility of the Processor that is not located within the borders of the EU.
B) The personal data was processed by a party that agreed to the draft processing contract the Controller sent, but did not yet sign it.
C) The system on which the personal data was processed was attacked causing damage to its storage devices.
D) There is a significant probability that the breach will lead to detrimental consequences for the privacy of the data subjects.

19 / 40
A Dutch controller has contracted the processing of sensitive personal data out to a processor in a North African country, without consulting the supervisory authority. Is was discovered and he was penalized by the supervisory authority. Six months later the authority finds out that the controller is guilty of the same transgression again for another processing operation.

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

A) € 750,000
B) €1,230,000
C) € 10,000,000 or 2% of the company's worldwide turnover, whichever is higher
D) € 20,000,000 or 4% of the company's worldwide turnover with a minimum of € 20,000,000 whichever is higher

20 / 40
Supervisory Authorities are assigned a number of responsibilities aimed at making sure data protection regulations are complied with.

What is one of those responsibilities?

A) Assessing codes of conduct for specific sectors relating to the processing of personal data.
B) Defining a minimum set of measures to be taken to protect personal data.
C) Investigation of all data breaches of which they have been notified.
D) Review of contracts and BCRs on compliance with the regulations.

21 / 40
A religious association wants to share personal data with their religious authority in a non-European country in order to comply with a legal request from the government concerned.

Which regulation in the GDPR applies in this case?

A) As an exception, processing of sensitive data revealing religious beliefs is permitted to a religious association.
B) It is not lawful to transfer personal data out of the EEA in response to a legal requirement from a third country.
C) Processing is lawful provided specific and unambiguous consent of the data subject has been acquired.
D) Processing personal data outside the EEA is permitted using the model contract clauses designed by the EU Commission.

22 / 40
On July 12, 2016 the European Commission implemented a ruling regarding transfer of personal data with the USA (EU-US Privacy Shield).

In terms of the GDPR, what kind of a ruling is this?

A) An adequacy decision
B) An exception decree
C) A standard binding contract
D) A treaty superseding the GDPR

23 / 40
Binding corporate rules are a means for organizations to ease their administrative burden when complying with the GDPR.

How do these rules help them?

A) They allow them to have underpinning contracts with all parties involved abroad.
B) They allow them to let third parties outside the European Economic Area process personal data.
C) They avoid the need to approach each supervisory authority in the EU separately.
D) They prevent them from having to ask a supervisory authority for permission for the processing of the data once their BCR are accepted.

24 / 40
In case a contractor contracts out the processing of personal data, the parties will enter into a written contract. This contract sets out subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects.

What other aspect must be governed by this written contract?

A) the accountability of the processor
B) the data breach notification obligation
C) the obligation that processors must co-operate with the supervisory authority
D) the obligations and rights of the controller

25 / 40
What should be done so that a Controller is able to outsource the processing of personal data to a Processor?

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 upon 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 all demands agreed upon in the Service Level Agreement (SLA) are met.

26 / 40
Data protection by design, as described in GDPR article 25, is based on seven basic principles. One of these is usually called *'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 its 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.

27 / 40
Often staff that works with personal data consider privacy and information security as separate issues.

Why is this wrong?

A) Privacy can't be guaranteed without identifying, implementing, and monitoring proper information security measures.
B) The supervisory authority expects the roles of data protection officer and Information security officer to be integrated.
C) The regulations identify specific information security measures that must be taken before handling personal data is allowed.

28 / 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 redesign of systems in a later stage.
B) The organization prevents non-compliance to the GDPR and minimizes the risk of fines.
C) The organization proves that it takes privacy seriously and aims for compliance to the GDPR.

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

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

30 / 40
What **best** describes the principle of data minimization?

A) Care must be taken to collect as little data as possible in order to protect the privacy and interests of the data subjects.
B) Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
C) In order to keep data manageable, it must be stored in such a manner that it requires a minimal amount of storage.
D) The number of items that is collected per data subject may not exceed the upper limit stated by the supervisory authority.

31 / 40
Session cookies are one of the most common types of cookie.

What **best** describes a session cookie?

A) It contains information on what you are doing, for instance the products you select in a web shop before you actually order.
B) It reveals your browse history, so other websites can find out which websites you have visited before you arrived there.
C) It stores your browse history, so you can trace where you have been on the net and revisit those site(s) if you want.
D) It collects your personal data, so the website can greet you by name and reuse your settings when you return.

32 / 40
Sometimes websites track visitors and store their information for marketing purposes.

Is the website obliged to notify the visitor that their information is being used for marketing purposes?

A) Yes
B) No

33 / 40
A company can present itself as an expert in a specific area of expertise making use of social media.

What is the **best** way to demonstrate expertise in a specific field?

A) By posting information about the company on Social Media.
B) By actively answering questions on Social Media about their product.
C) By posting about how the product of the competitor is inferior to that of the company.
D) By posting about new products the company is developing.

34 / 40
A security breach has occurred in an information system that also holds personal data.

What is the **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 with the relevant supervisory authority.

35 / 40
The word 'privacy' is not mentioned in the GDPR.

How is 'privacy' related to 'data protection'?

A) Data protection is a set of rules and regulations on processing personal data. Privacy is the result of data protection.
B) Privacy is the right to be protected from interference in personal matters. Data protection is the means to implement that protection.
C) Privacy is the right to keep personal matters secret. Data protection is the right to keep personal data secret.
D) The terms 'privacy' and 'data protection' are interchangeable. There is no real difference in meaning.

36 / 40
Regulation (EU) 2016/679, known as the GDPR, repeals an earlier EU Directive.

Which directive is being repealed (replaced)?

A) Directive 2002/58/EC of 12 July 2002
B) Directive 2006/24/EC of 15 March 2006
C) Directive 95/46/EC of 24 October 1995
D) Directive 97/66/EC of 15 December 1997

37 / 40
Which right of data subjects 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 without any cost for the data subject.
C) Personal data must be always changed at the request of the data subject.
D) Personal data must be erased at all times if a data subject requests this.

38 / 40
The GDPR distinguishes 'sensitive personal data' as a special category of personal data.

What is an example of such data?

A) An appointment in a hospital with a medical specialist
B) An International Bank Account Number (IBAN)
C) Subscription to a scientific journal for politics
D) The membership of a branch association

39 / 40
Which role in data protection determines the purposes and means of the processing of personal data?

A) Controller
B) Data Protection Officer
C) Processor

40 / 40
Which information is regarded as personal data according to the GDPR?

A) Information about a person, which might harm the privacy of that person, even when untrue
B) Any information regarding an identifiable natural person
C) Information, regarding an identifiable natural person, which is digitalized

Answer Key

1 / 40
The illegal collection, storage, modification, disclosure or dissemination of personal data is an offence by European law.

What kind of offence is this?

A) a content related offence
B) an economic offence
C) an intellectual property offence
D) a privacy offence

A) Incorrect. A content related offence concerns dissemination of racist statements, (child) pornography or information inciting violence.
B) Incorrect. Economic offences relate to unauthorized access to systems (hacking, distribution of viruses, etc.) computer espionage, -forgery, and - fraud).
C) Incorrect. Intellectual property offences pertain to violations of copyright and related rights.
D) Correct. Any illegal processing of personal data is an offence. No Source: basic knowledge.

2 / 40
How are privacy and data protection related to each other?

A) Data protection is a subset of privacy.
B) Privacy is a subset of data protection.
C) They are the same thing.
D) You cannot have privacy without data protection.

A) Incorrect. Privacy spans a lot of concepts like spatial, relational, bodily and information privacy. Data protection has no relation to some of these.
B) Incorrect. Privacy spans a lot of concepts like spatial, relational, bodily and information privacy. Data protection helps to guarantee some of these.
C) Incorrect. Data protection for example has nothing to do with spatial privacy.
D) Correct. Data protection is a necessary measure to protect the fundamental right to privacy. Source: White Paper – Privacy, Personal Data and the GDPR - §1.3 Definitions

3 / 40
What is the GDPR **mainly** intended for?

A) To be a common ground upon which the member states can build their own laws.
B) To make non-EU countries respect the right to privacy of individuals within the EU.
C) To secure privacy as a fundamental human right for everyone.
D) To strengthen and unify data protection for individuals within the EU.

A) Incorrect. The GDPR is a regulation, meaning it will repeal the data protection laws in the member's states.
B) Incorrect. Its main objective is aimed at defining the data protection rights of individuals within the EU.
C) Incorrect. The GDPR does explicitly state data protection is a fundamental right, but its scope is limited to individuals within the EU.
D) Correct. The scope of the GDPR is limited to data protection as a right of individuals within the EU and aims to harmonize the rules for that within the EU. Source: EU GDPR, A pocket guide – Introduction.

4 / 40
The GDPR is related to personal data protection.

What is the definition of personal data?

A) any information relating to an identified or identifiable natural person
B) any information that the European citizens would like to protect
C) data that directly or indirectly reveal someone's racial or ethnic background, religious views, and data related to health or sexual habits
D) preservation of confidentiality, integrity and availability of information

A) Correct. This is the official definition of the data protection. Source: EU GDPR, A pocket guide - Chapter 2 Terms and definitions GDPR 2016/679 Article 4: definition
B) Incorrect. This definition is too generic.
C) Incorrect. This is the definition of sensitive data not of generic personal data.
D) Incorrect. This is the definition of information security from ISO/IEC 27000:2014.

5 / 40
According to the GDPR, which personal data category is regarded as sensitive data?

A) credit card details
B) trade union membership
C) passport number
D) social security number

A) Incorrect. Credit card details are not sensitive data according to the GDPR.
B) Correct. Membership of a trade union is sensitive data. Source: GDPR art. 9, rec.10 - Special categories of personal data.
C) Incorrect. Passport details are not sensitive data according to the GDPR.
D) Incorrect. A social security number is not sensitive data according to the GDPR.

6 / 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 data is being shared on social media or transferred by email or otherwise through the Internet
D) Only operations in which the personal data is used for the purposes for which it was collected

A) Correct. Source: GDPR art.4 (2)
B) Incorrect. 'processing' means any operation which is performed on personal data.
C) Incorrect. 'processing' means any operation which is performed on personal data.
D) Incorrect. 'processing' means any operation which is performed on personal data.

7 / 40
"An independent public authority which is established by a Member State pursuant to Article 51."

Which role in data protection is defined?

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

A) Incorrect.
See Regulation 2016/679, Article 4.
B) Incorrect.
See Regulation 2016/679, Article 4.
C) Correct. Source: GDPR 2016/679, Article 4 and Article 51.
D) Incorrect.
See Regulation 2016/679, Article 4.

8 / 40
'Informed consent' is a lawful basis to process personal data under the GDPR. The purpose of the processing for which consent is given should be documented.

At what time in the process should the data subject's consent be obtained?

A) After the purpose specification is presented and before personal data is collected.
B) Before the purpose specification is conceived and presented.
C) Before the personal data is processed.
D) Before the personal data is published or disseminated.

A) Correct. Consent can only be informed after the purpose specification is presented to the data subject. Source: GDPR recitals (32), (42).
B) Incorrect. Consent can only be informed after the purpose specification is presented to the data subject.
C) Incorrect. Collection of personal data is 'processing' and as such needs informed consent of the data subject.
D) Incorrect. Publishing and dissemination of personal data are 'processing' and as such need informed consent of the data subject.

9 / 40
The GDPR is based on the principles of proportionality and subsidiarity.

What is the meaning of 'proportionality' in this context?

A) Personal data can only be processed in accordance with the purpose specification.
B) Personal data cannot be re-used without explicit and informed consent.
C) Personal data may only be processed in case 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) Incorrect. This is the definition of subsidiarity.
D) Correct. Source: White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity & GDPR art. 35 (7)

10 / 40
The processing of personal data has to meet certain quality requirements.

What is one of these quality requirements defined by the GDPR?

A) The data processed must be archived.
B) The data processed must be encrypted.
C) The data processed must be indexed.
D) The data processed must be relevant.

A) Incorrect. No such requirement is defined by the GDPR.
B) Incorrect. No such requirement is defined by the GDPR.
C) Incorrect. No such requirement is defined by the GDPR.
D) Correct. This requirement is defined by the GDPR. Source: White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity

11 / 40
Every time personal data is processed proportionality and subsidiarity must be checked.

What is the requirement for the personal data being processed?

A) It must be limited always to what is necessary to achieve the defined goals and must be limited to the least “intrusive” data.
B) It must be handled by the smallest number of employees possible and they must work for the Controller or an affiliate.
C) It must be limited to a predefined storage size and the system used must be financed by the Controller.
D) It must be used for the smallest number of purposes possible and this may not be done outside the premises of the Processor.

A) Correct. These terms mean you collect no more data than needed to achieve the predefined goal(s), and you always try to use data that has the least impact on the privacy of the Data Subject. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Lawful processing
B) Incorrect. The number of employees or their affiliation to some subsidiary has nothing to do with these terms.
C) Incorrect. Storage size and who finances the systems used has nothing to do with these terms.
D) Incorrect. As long as the Data Subject gives consent the number of goals is not explicitly restricted, nor is the location.

12 / 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?

A) Compliance
B) Data protection by default
C) Privacy by design
D) Embedded protection

A) Incorrect. Compliance is the state or fact of according with - or 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. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data protection by design and by default & GDPR art. 20 (2).
C) Incorrect. Data protection by design refers to a design that includes appropriate measures to implement data protection principles.
D) Incorrect. Embedded data protection is the result of data protection by design.

13 / 40
What is the term used in the GDPR for unauthorized disclosure of, or access to, personal data?

A) Confidentiality violation
B) Data breach
C) Incident
D) Security incident

A) Incorrect. GDPR uses the term data breach. Not every data breach is a confidentiality violation.
B) Correct. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches & GDPR article 4 (12)
C) Incorrect. GDPR uses the term data breach. Not every incident is a data breach.
D) Incorrect. GDPR uses the term data breach. Not every security incident is a data breach.

14 / 40
It has been ascertained that a data breach of sensitive personal data occurred.

To whom must this ultimately be reported according to the GDPR?

A) the supervisory authority
B) the Data Protection Officer (DPO)
C) the manager of the department
D) the police

A) Correct. Data breaches must be reported to the DPA if they might have a significant impact on the security of the data subject or their personal data. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation Data breaches & GDPR article 4 (12)
B) Incorrect. Even though it might be reported to an internal DPO, in the end it must be reported to the DPA.
C) Incorrect. Even though it might be reported to the manager, in the end it must be reported to the DPA.
D) Incorrect. Data breaches do not necessarily have to be reported to the police, but in the end they must be reported to the DPA.

15 / 40
While performing a backup, a data server disk crashes. Both the data and the backup are lost. The disk contained personal data but no sensitive data.

What kind of incident is this?

A) data breach
B) security breach
C) security incident

A) Correct. Personal data irretrievably lost is regarded as unauthorized processing, which makes it a data breach. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches & GDPR Chapter I, Article 4, Definitions.
B) Incorrect. Personal data irretrievably lost is regarded as unauthorized processing, which makes it a data breach.
C) Incorrect. Personal data irretrievably lost is regarded as unauthorized processing, which makes it a data breach.

16 / 40
Someone working for a trade union took a draft newsletter for the members home to finish it there. The USB stick containing the draft and the mailing list, was lost.

To whom, among others, should this data breach be reported?

A) all members on the mailing list
B) the board of the trade union
C) the police

A) Correct. This is sensitive data, so the loss must be reported to both the privacy authority and the data subjects. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches
B) Incorrect. This is sensitive data, so the loss must be reported to both the privacy authority and the data subjects.
C) Incorrect. This is sensitive data, so the loss must be reported to both the privacy authority and the data subjects.

17 / 40
A social services organization plans to design a new database to administrate its clients and the care they need.

In order to request permission with the supervisory authority, what is one of the first important steps to be taken?

A) Collect data about the clients and the amount and kind of care needed and provided.
B) Conduct a data protection impact assessment (DPIA) to assess the risks of the intended processing.
C) Obtain consent of the clients for the intended processing of their personal data.

A) Incorrect. Collecting medical personal data is by definition 'processing sensitive data'. Permission of the DPA and the data subject is needed beforehand.
B) Correct. When asking consent to process data, the data subject 'should be made aware of risks, rules, safeguards and rights ...' Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Consent & GDPR recital (39).
C) Incorrect. When asking consent to process data, the data subject 'should be made aware of risks, rules, safeguards and rights ...' A PIA is needed first to assess those risks and safeguards.

18 / 40
In which case should the data subjects always be notified of a data breach?

A) The personal data was processed at a facility of the Processor that is not located within the borders of the EU.
B) The personal data was processed by a party that agreed to the draft processing contract the Controller sent, but did not yet sign it.
C) The system on which the personal data was processed was attacked causing damage to its storage devices.
D) There is a significant probability that the breach will lead to detrimental consequences 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 data breaches.
B) Incorrect. Personal data processed by another party than the controller without a valid written contract is considered a 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. Source: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs.

19 / 40
A Dutch controller has contracted the processing of sensitive personal data out to a processor in a North African country, without consulting the supervisory authority. Is was discovered and he was penalized by the supervisory authority. Six months later the authority finds out that the controller is guilty of the same transgression again for another processing operation.

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

A) € 750,000
B) €1,230,000
C) € 10,000,000 or 2% of the company's worldwide turnover, whichever is higher
D) € 20,000,000 or 4% of the company's worldwide turnover with a minimum of € 20,000,000 whichever is higher

A) Incorrect. According to GDPR art. 83.3 the maximum fine is 4% of the company's worldwide turnover with a minimum of € 20.000.000.
B) Incorrect. According to GDPR art. 83.3 the maximum fine is 4% of the company's worldwide turnover with a minimum of € 20.000.000.
C) Incorrect. According to GDPR art. 83.3 the maximum fine is 4% of the company's worldwide turnover with a minimum of € 20.000.000
D) Correct. This is the maximum for a violation. Source: White Paper – Privacy, Personal Data and the GDPR - §7.3.3 General conditions for imposing administrative fines.

20 / 40
Supervisory Authorities are assigned a number of responsibilities aimed at making sure data protection regulations are complied with.

What is one of those responsibilities?

A) Assessing codes of conduct for specific sectors relating to the processing of personal data.
B) Defining a minimum set of measures to be taken to protect personal data.
C) Investigation of all data breaches of which they have been notified.
D) Review of contracts and BCRs on compliance with the regulations.

A) Correct. One of the responsibilities of DPAs is to provide general advice on how to comply with the regulations. Source: White Paper – Privacy, Personal Data and the GDPR - §7.1.4 To set standards.
B) Incorrect. A Supervisory Authority will give general advice on what they consider an appropriate level of security. They will however not tell you what specific measures you need to take to achieve that level. Even if they want to they would not be able to, because there simply is no one-size-fits-all solution.
C) Incorrect. DPAs do not have the obligation, nor the capacity to investigate all breaches they know of. But they will investigate those they deem significant or noteworthy.
D) Incorrect. A DPA is not a legal counsel. They do not review contracts or Binding Corporate Rules. However, in the course of an investigation they might take a look at a specific contract or set of BCRs.

21 / 40
A religious association wants to share personal data with their religious authority in a non-European country in order to comply with a legal request from the government concerned.

Which regulation in the GDPR applies in this case?

A) As an exception, processing of sensitive data revealing religious beliefs is permitted to a religious association.
B) It is not lawful to transfer personal data out of the EEA in response to a legal requirement from a third country.
C) Processing is lawful provided specific and unambiguous consent of the data subject has been acquired.
D) Processing personal data outside the EEA is permitted using the model contract clauses designed by the EU Commission.

A) Incorrect. Religious associations are permitted to process personal data relating to their former and current members, *but it is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country.*
B) Correct. Source: White Paper – Privacy, Personal Data and the GDPR - §7.5.2 Regulations applying to data transfer outside the EEA & EU GDPR, A pocket guide - Chapter 3: The regulation – International transfers & GDPR art. 48.
C) Incorrect. It is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country, *not even with consent of the data subject.*
D) Incorrect. Processing of sensitive data outside EU can be lawful, but not in response to a request from a third country government.

22 / 40
On July 12, 2016 the European Commission implemented a ruling regarding transfer of personal data with the USA (EU-US Privacy Shield).

In terms of the GDPR, what kind of a ruling is this?

A) An adequacy decision
B) An exception decree
C) A standard binding contract
D) A treaty superseding the GDPR

A) Correct. The ruling is an adequacy decision in accordance with the GDPR regarding processing in 3rd countries. Source: White Paper – Privacy, Personal Data and the GDPR - §7.5.4 Regulations applying to data transfer between the EEA and the USA & EU GDPR, A pocket guide - Chapter 3 The Regulation – International transfers & GDPR recitals 104 and 106.
B) Incorrect. An exception is about transfers essential to respond to terrorist offences or serious crimes (art. 11)
C) Incorrect. The ruling is an adequacy decision in accordance with the GDPR regarding processing in 3rd countries.
D) Incorrect. The ruling is an adequacy decision in accordance with the GDPR regarding processing in 3rd countries.

23 / 40
Binding corporate rules are a means for organizations to ease their administrative burden when complying with the GDPR.

How do these rules help them?

A) They allow them to have underpinning contracts with all parties involved abroad.
B) They allow them to let third parties outside the European Economic Area process personal data.
C) They avoid the need to approach each supervisory authority in the EU separately.
D) They prevent them from having to ask a supervisory authority for permission for the processing of the data once their BCR are accepted.

A) Incorrect. BCRs are drafted so organizations do not have to use written underpinning contracts for each affiliate separately.
B) Incorrect. BCRs are valid within an organization and all its affiliates only. They do not apply to other parties.
C) Correct. Once BCRs are approved by one DPA inside the EU you do not have to ask the other DPAs inside the EU to approve them anymore. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Binding corporate rules
D) Incorrect. BCR must be authorized by a DPA too.

24 / 40
In case a contractor contracts out the processing of personal data, the parties will enter into a written contract. This contract sets out subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects.

What other aspect must be governed by this written contract?

A) the accountability of the processor
B) the data breach notification obligation
C) the obligation that processors must co-operate with the supervisory authority
D) the obligations and rights of the controller

A) Incorrect. This is a direct obligation of the GDPR to processors.
B) Incorrect. This is a direct obligation of the GDPR to processors.
C) Incorrect. This is a direct obligation of the GDPR to processors.
D) Correct. This is a direct obligation of the GDPR to processors. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts & GDPR art. 28 (3).

25 / 40
What should be done so that a Controller is able to outsource the processing of personal data to a Processor?

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 upon 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 all demands agreed upon in the Service Level Agreement (SLA) are met.

A) Incorrect. You do not have to the DPA ask for permission for each instance of outsourcing.
B) Incorrect. The DPA 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 in which the Controller defines the goals and means of processing. Both parties must sign this contract. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts & GDPR art. 28 (3).
D) Incorrect. An SLA is not enough as it will focus on operations, not necessarily on defining goals.

26 / 40
Data protection by design, as described in GDPR article 25, is based on seven basic principles. One of these is usually called *'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 its 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. Privacy by Design rejects the approach that Privacy has to compete with other legitimate interests, design objectives, and technical capabilities. All objects need to be accommodated in a positive-sum "win-win" manner.
C) Correct, this is the essence. Source: White Paper – Privacy, Personal Data and the GDPR - § 8.1.1 The seven principles of data protection by design & GDPR art 25
D) Incorrect. This is an aspect of 'privacy *embedded* into design', one of the other six basic principles

27 / 40
Often staff that works with personal data consider privacy and information security as separate issues.

Why is this wrong?

A) Privacy can't be guaranteed without identifying, implementing, and monitoring proper information security measures.
B) The supervisory authority expects the roles of data protection officer and Information security officer to be integrated.
C) The regulations identify specific information security measures that must be taken before handling personal data is allowed.

A) Correct. Privacy and Data Protection are about guaranteeing confidentiality of personal data a.o. This requires the implementation of security measures. Source: White Paper – Privacy, Personal Data and the GDPR - § 2.1.6 - integrity and confidentiality.
B) Incorrect. The DPA does not expect these roles to be integrated at all.
C) Incorrect. The regulations specify goals that must be met, but no specific measures that must be taken.

28 / 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 redesign of systems in a later stage.
B) The organization prevents non-compliance to the GDPR and minimizes the risk of fines.
C) The organization proves that it takes privacy seriously and aims for compliance to the GDPR.

A) Incorrect. This aspect may strengthen the confidence of management, but not customers or citizens.
B) Incorrect. Preventing fines may strengthen the confidence of management, but not customers or citizens.
C) Correct. Source: EU GDPR, A pocket guide - Chapter 3 The Regulation - Data Protection Impact Assessments

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

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

A) Incorrect. The audit is not the implementation of the measures, but an assessment of the effectiveness of them.
B) Correct. According to the GDPR this is an important task of the DPA as supervising authority. Source: GDPR art 57.1(a)
C) Incorrect. The DPA has the task to monitor compliance and to advice on enhancements, but its purpose is not to protect the controller.

30 / 40
What **best** describes the principle of data minimization?

A) Care must be taken to collect as little data as possible in order to protect the privacy and interests of the data subjects.
B) Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
C) In order to keep data manageable, it must be stored in such a manner that it requires a minimal amount of storage.
D) The number of items that is collected per data subject may not exceed the upper limit stated by the supervisory authority.

A) Incorrect. As a matter of fact, the GDPR states the data collected must be adequate, implying it does not have to be the absolute minimum.
B) Correct. This is the very definition of data minimization. It is aimed at making sure only the data needed to achieve the defined goals are collected. Source: White Paper – Privacy, Personal Data and the GDPR - §2.1 Data processing principles & GDPR article 5.1.c.
C) Incorrect. Storage size has nothing to do with this principle.
D) Incorrect. DPAs do not set an upper limit on the number of items collected as long as they are limited to those needed to achieve the defined goals.

31 / 40
Session cookies are one of the most common types of cookie.

What **best** describes a session cookie?

A) It contains information on what you are doing, for instance the products you select in a web shop before you actually order.
B) It reveals your browse history, so other websites can find out which websites you have visited before you arrived there.
C) It stores your browse history, so you can trace where you have been on the net and revisit those site(s) if you want.
D) It collects your personal data, so the website can greet you by name and reuse your settings when you return.

A) Correct. A session cookie is kept in memory to save information on the session. It is erased when you close the session. Source: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrect. A session cookie is erased when you close the session, so it cannot be used in a next session.
C) Incorrect. A session cookie is erased when you close the session, so it cannot be used in a next session.
D) Incorrect. A session cookie is erased when you close the session, so it cannot be used in a next session.

32 / 40
Sometimes websites track visitors and store their information for marketing purposes.

Is the website obliged to notify the visitor that their information is being used for marketing purposes?

A) Yes
B) No

A) Correct. The website has the obligation to notify the visitor that their information is being used for marketing purposes. They have the right to object to processing of personal data concerning him or her for marketing purposes. Source: White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrect. The website has the obligation to notify the visitor that their information is being used for marketing purposes. They have the right to object to processing of personal data concerning him or her for marketing purposes.

33 / 40
A company can present itself as an expert in a specific area of expertise making use of social media.

What is the **best** way to demonstrate expertise in a specific field?

A) By posting information about the company on Social Media.
B) By actively answering questions on Social Media about their product.
C) By posting about how the product of the competitor is inferior to that of the company.
D) By posting about new products the company is developing.

A) Incorrect. Just posting info about the company does not make you an expert in a field.
B) Correct. Answering (and actively answering) questions about a specific product on social media could make your company an expert. Source: White Paper – Privacy, Personal Data and the GDPR - § 8.6. Practice related applications of the use of data, marketing and social media.
C) Incorrect. This is just bragging about how good your product is (and maybe it isn't).
D) Incorrect. This is just showing that you as a company are developing new products and yes, it can help improve sales but it does not make the company an expert.

34 / 40
A security breach has occurred in an information system that also holds personal data.

What is the **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 with the relevant supervisory authority.

A) Correct. Source: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs.
B) Incorrect. A PIA is conducted when designing personal data processing operations.
C) Incorrect. The controller must first ascertain whether the incident is a data breach that needs to be reported.
D) Incorrect. The controller must first ascertain whether the incident is a data breach that needs to be reported.

35 / 40
The word 'privacy' is not mentioned in the GDPR.

How is 'privacy' related to 'data protection'?

A) Data protection is a set of rules and regulations on processing personal data. Privacy is the result of data protection.
B) Privacy is the right to be protected from interference in personal matters. Data protection is the means to implement that protection.
C) Privacy is the right to keep personal matters secret. Data protection is the right to keep personal data secret.
D) The terms 'privacy' and 'data protection' are interchangeable. There is no real difference in meaning.

A) Incorrect. Privacy is a right, data protection is the means to ensure it.
B) Correct. Source: White Paper – Privacy, Personal Data and the GDPR - § 1.3 Definitions.
C) Incorrect. Privacy is a right, data protection is the means to ensure it.
D) Incorrect. Privacy is a right, data protection is the means to ensure it.

36 / 40
Regulation (EU) 2016/679, known as the GDPR, repeals an earlier EU Directive.

Which directive is being repealed (replaced)?

A) Directive 2002/58/EC of 12 July 2002
B) Directive 2006/24/EC of 15 March 2006
C) Directive 95/46/EC of 24 October 1995
D) Directive 97/66/EC of 15 December 1997

A) Incorrect. Directive 2002/58/EC amends some parts of Directive 97/66/EC.
B) Incorrect. This directive is about the retention of data collected for instance by internet providers.
C) Correct. This replacement is mentioned in the (sub) title of the regulation. Source: GDPR.
D) Incorrect. This Directive complements directive 95/46/EC to ensure an equivalent level of protection of fundamental rights and freedoms in the member states.

37 / 40
Which right of data subjects 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 without any cost for the data subject.
C) Personal data must be always changed at the request of the data subject.
D) Personal data must be erased at all times if a data subject requests this.

A) Incorrect. It has to be provided in a structured, commonly used and machine-readable format, but not necessarily in any format the Data Subject specifies.
B) Correct. However only the first copy has to be provided free of cost. Source: EU GDPR, A pocket guide – Chapter 3 The Regulation – Data subjects' rights.
C) Incorrect. Only erroneous data has to be rectified.
D) Incorrect. Article 17 gives some exceptions to this like when the data is needed for the establishment, exercise or defense of legal claims.

38 / 40
The GDPR distinguishes 'sensitive personal data' as a special category of personal data.

What is an example of such data?

A) An appointment in a hospital with a medical specialist
B) An International Bank Account Number (IBAN)
C) Subscription to a scientific journal for politics
D) The membership of a branch association

A) Correct. An appointment with a medical specialist is 'personal data concerning health'. See GDPR art. 9.1.
B) Incorrect. An IBAN is data uniquely related to a person, i.e. personal data. But not sensitive personal data according to GDPR art. 9.
C) Incorrect. A scientific journal for politics is not 'personal data revealing political opinions, religious or philosophical beliefs' and as such not sensitive personal data according to GDPR art. 9.
D) Incorrect. Only trade union membership and other personal data 'revealing (…) political opinions, religious or philosophical beliefs' is sensitive personal data according to GDPR art. 9.

39 / 40
Which role in data protection determines the purposes and means of the processing of personal data?

A) Controller
B) Data Protection Officer
C) Processor

A) Correct. Controller: the 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. Source: White Paper – Privacy, Personal Data and the GDPR - §1.4 Roles, responsibilities, stakeholders.
B) Incorrect.
C) Incorrect.

40 / 40
Which information is regarded as personal data according to the GDPR?

A) Information about a person, which might harm the privacy of that person, even when untrue
B) Any information regarding an identifiable natural person
C) Information, regarding an identifiable natural person, which is digitalized

A) Incorrect. Any statement about an identifiable natural person is personal data according to the GDPR.
B) Correct. Source: EU GDPR, A pocket guide – Chapter 2 Term and definitions - Personal data & GDPR art.4 (1).
C) Incorrect. Any statement about an identifiable natural person is personal data according to the GDPR.

Evaluation

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

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

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER