Sample Exam

Edition 201810

Content

Introduction

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

This exam consists of 20 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 20. Each correct answer is worth one point. If you obtain 13 points or more you will pass.

The time allowed for this exam is 30 minutes.

Good luck!

Sample Exam

1 / 20
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 / 20
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 / 20
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.

4 / 20
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 / 20
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

6 / 20
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.

7 / 20
"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 / 20
Which role in data protection determines the purposes and means of the processing of personal data?

A) Controller
B) Data Protection Officer
C) Processor

9 / 20
'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.

10 / 20
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 / 20
"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

12 / 20
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

13 / 20
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.

14 / 20
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

15 / 20
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.

16 / 20
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.

17 / 20
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.

18 / 20
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.

19 / 20
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.

20 / 20
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

Answer Key

1 / 20
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 / 20
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 / 20
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.

4 / 20
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 / 20
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.

6 / 20
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.

7 / 20
"*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 / 20
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.

9 / 20
'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.

10 / 20
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 / 20
"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.

12 / 20
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.

13 / 20
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.

14 / 20
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.

15 / 20
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 don't 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 don't 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.

16 / 20
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 don't 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.

17 / 20
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 don't 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.

18 / 20
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.

19 / 20
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.

20 / 20
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.

Evaluation

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

Question	Anwer	Question	Answer
1	D	**11**	B
2	D	**12**	B
3	B	**13**	B
4	A	**14**	D
5	B	**15**	A
6	B	**16**	C
7	C	**17**	C
8	A	**18**	A
9	A	**19**	A
10	D	**20**	A

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER