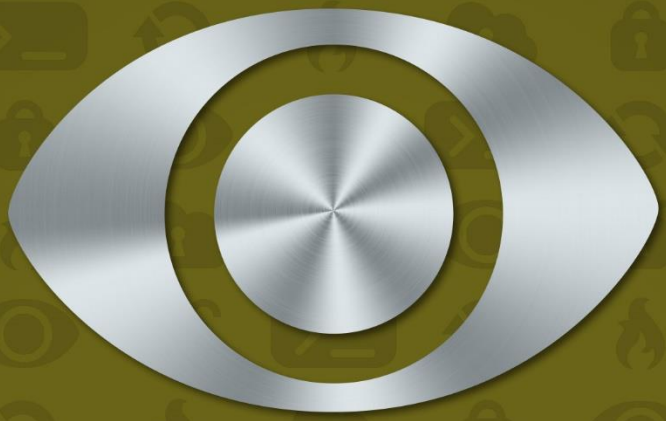

PRIVACY & DATA PROTECTION

FOUNDATION

Sample Exam

SECO INSTITUTE

General Information

The SECO-Institute offers its official Cyber Security & Governance courseware through accredited training centres where students are trained by accredited instructors. Exam candidates can take their exams at one of the accredited exam centres or directly with the SECO-Institute.

Attending a course is not a prerequisite for taking an exam. Upon successful completion of a foundation exam (with a passing score of 60%), candidates can claim their digital badge at the SECO-Institute.

This Sample Exam allows candidates to familiarise themselves with the structure and topic areas of the current Privacy & Data Protection Foundation examination. It is recommended to take the Sample Exam before registering for the certification exam. The results of the Sample Exam do not count towards the certification assessment.

Examination type

- Computer-based
- 40 Multiple choice: 2,5 points per question

Time allotted for examination

- 60 minutes

Examination details

- Pass mark: 60% (60 points out of a total of 100)
- Open book/notes: no
- Electronic equipment permitted: no
- The Rules and Regulations for SECO-Institute examinations apply to this exam

Questions

Question 1

Which European Union (EU) legal document forms the basis for all EU privacy and data protection legislation?

A. UN Universal Declaration of Human Rights
B. DIRECTIVE 95/46/EC
C. EU Charter of Fundamental Rights
D. General Data Protection Regulation

Question 2

The GDPR does not describe the concept of 'privacy'. Which European Union (EU) legal document contains an Article 7 on the right to 'respect for private and family life'?

A. EU Charter of Fundamental Rights
B. DIRECTIVE 95/46/EC
C. General Data Protection Regulation
D. DIRECTIVE 2016/680

Question 3

Which legal document is considered the cornerstone of all privacy legislation?

A. European Convention on Human Rights
B. EU Charter of Fundamental Rights
C. Universal Declaration of Human Rights
D. EC Implementing Decision 2016-7-12 (EU-US Privacy Shield)

Question 4

Which EU legal instrument applies directly to all Member States?

A. Directive
B. Decision
C. Executive order
D. Regulation

Question 5

The GDPR defines a certain data protection role as "... 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." Which role is this?

A. Processor
B. Controller
C. Supervisory authority
D. Data protection officer

Question 6

Which body monitors the processing of personal data by EU institutions?

A. European Data Protection Board
B. European Data Protection Supervisor
C. Independent supervisory authority
D. Article 29 Working Party

Question 7

What do we call those parts of the GDPR that explain the reasoning behind the provisions and provide us with complementary information?

A. Citations
B. Articles
C. General provisions
D. Recitals

Question 8

Which of the following activities falls within the GDPR's material scope?

A. Member States carrying out activities for the Common Foreign and Security Policy
B. Processing of personal data wholly or partly by automated means
C. Processing of personal data by natural persons in the course of a purely personal or household activity
D. Processing of personal data by competent authorities for crime prevention

Question 9

Chapter I of the GDPR contains general provisions. Within Chapter I, which article describes that the GDPR does not apply to personal data processing by natural persons in the course of a purely personal or household activity?

A. Article 2 Material scope
B. Article 3 Territorial scope
C. Article 4 Definitions
D. Article 1 Subject-matter and objectives

Question 10

What is the territorial scope of the GDPR?

A. EU
B. EEA
C. EFTA
D. UN

Question 11

Which data are NOT considered 'personal data' under the GDPR?

A. Sensitive data
B. Pseudonymised personal data
C. Anonymised personal data
D. Biometric data

Question 12

Which concept does the GDPR define as "any operation or set of operations which are performed on personal data"?

A. Controlling
B. Purpose limitation
C. Processing
D. Storage limitation

Question 13

Which activity falls outside the scope of the GDPR?

A. Profiling
B. Storing anonymised personal data
C. Storing any type of personal data
D. Erasure of personal data

Question 14

Which processing principle requires the personal data to be up to date?

A. Accuracy
B. Purpose limitation
C. Storage limitation
D. Integrity and confidentiality

Question 15

Which processing principle requires the controller to explicitly describe the reason for which the data will be processed?

A. Purpose limitation
B. Integrity and confidentiality
C. Data minimisation
D. Storage limitation

Question 16

Who can obtain restriction of processing?

A. Controller
B. Processor
C. Representative
D. Data subject

Question 17

In which situation may the controller process sensitive data?

A. The data are necessary for marketing purposes
B. The data subject has made the data public
C. The data are archived by the controller
D. The data are only stored but not actively used by the controller

Question 18

The GDPR allows Member States to maintain or introduce further conditions with regard to the processing of certain categories of personal data. Which is an example of those categories of personal data?

A. Data concerning a person's health
B. Data concerning a person's economic situation
C. Data concerning a person's personal preferences
D. Data concerning a person's location

Question 19

In certain areas, Member States may adopt exemptions and derogations from specific provisions of the GDPR. For which type of processing may Member States adopt exemptions and derogations?

A. Processing by clubs and cultural associations
B. Processing of anonymised personal data
C. Processing by churches and religious associations
D. Processing of pseudonymised personal data

Question 20

Which right enables the data subject to have inaccurate personal data corrected by the controller?

A. The right to rectification
B. The right to data portability
C. The right to restriction of processing
D. The right to withdraw consent

Question 21

A controller informs a data subject that her personal data is no longer necessary and will be erased. The data subject opposes the erasure and requests the restriction of processing instead. After the processing has been restricted, what purpose can the personal data be used for?

A. The establishment, exercise or defence of legal claims
B. Archiving purposes
C. Transfer of the data to another controller
D. Journalistic purposes

Question 22

According to the GDPR, which is NOT a legitimate reason for transferring personal data to 'third countries'?

A. The transfer is covered by binding corporate rules
B. The transfer is demanded by a US presidential order
C. The third country has received an adequacy decision from the European Commission
D. The controller has provided appropriate safeguards

Question 23

The GDPR requires the implementation of appropriate technical and organisational security measures. Who bears ultimate responsibility for implementing the security measures?

A. The processor
B. The independent supervisory authority
C. The data subject
D. The controller

Question 24

Which is NOT one of the 7 foundational principles of privacy by design and by default?

A. Integrity and confidentiality
B. Visibility and transparency
C. Privacy embedded
D. Full functionality, positive sum

Question 25

A software company takes data protection aspects into account when developing applications. What do we call this approach?

A. Data protection by default
B. Legitimate data protection
C. Data protection by design
D. Organisational data protection

Question 26

Both the controller and the processor are required to create and maintain records of their processing activities. Which is a mandatory element of the processor’s record?

A. A description of the categories of data subjects
B. A description of the envisaged retention periods
C. A description of the technical and organisational security measures
D. The purposes of the processing

Question 27

The GDPR requires (the representatives of) controllers and processors to "cooperate with the supervisory authority in the performance of its tasks". This includes making the records of processing activities available to the supervisory authority. Which statement is true about the obligation to make the records available to the supervisory authority?

A. The controller/processor must submit every new record to the supervisory authority
B. The controller/processor must disclose the records on request of the supervisory authority
C. The controller/processor must disclose the records where required by national law
D. The controller/processor should seek advice from the European Data Protection Board before making a record available to the supervisory authority

Question 28

Which activity can be performed without carrying out a Data Protection Impact Assessment (DPIA)?

A. Systematic monitoring of public areas on a large scale
B. Systematic extensive evaluation of personal aspects
C. Processing with new technologies
D. Processing for the establishment, exercise or defence of legal claims

Question 29

Finish the sentence: Transparency is an essential requirement in the controller's communications with ...

A. The data subject, the recipients of the personal data and the supervisory authority
B. The data subject, the processor and the supervisory authority
C. The processor, the recipients of the personal data and the Data Protection Officer
D. The processor and the sub-processors

Question 30

What does "transparent" communication mean?

A. Concise
B. Intelligible
C. Clear and plain language
D. All of the above

Question 31

In which case must the controller inform the data subject of a personal data breach?

A. The breach has resulted in the loss of encrypted personal data
B. The breach involved personal data that had been rectified
C. The breach is likely to result in a high risk to the rights and freedoms of the data subject
D. The data subject had withdrawn consent to the processing before the breach occurred

Question 32

A controller has erased personal data. In which case is the controller exempt from the obligation to notify every recipient of the erasure?

A. The processing was based on the data subject's explicit consent
B. The personal data were inaccurate
C. Notifying the recipients would involve disproportionate effort
D. The erasure is irreversible

Question 33

In which case must the controller consult the supervisory authority prior to the processing?

A. A new processor has adopted the binding corporate rules
B. A data subject has evoked his/her right of access
C. The controller has suffered several data breaches in the past
D. The results of the Data Protection Impact Assessment indicate that the processing involves a high risk that cannot be mitigated by the controller

Question 34

In which case must the controller notify the supervisory authority?

A. A security incident occurs and the incident involves personal data
B. A security incident leads to the accidental loss of personal data
C. A risk analysis indicates that there are vulnerabilities in the processing system
D. A data subject withdraws consent to the processing

Question 35

Which statement is true about the data breach notification obligation?

A. The supervisory authority must be notified only if the breach is likely to have serious adverse effects on the affected data subjects
B. The supervisory authority must be notified only if the data were not encrypted
C. The supervisory authority must be notified only if the breach is likely to result in a risk to the rights and freedoms of natural persons
D. The supervisory authority must be notified of all breaches, unless the controller can demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons

Question 36

What does the term 'accountability' mean in the GDPR?

A. The obligation to be able to demonstrate compliance with the GDPR
B. The obligation to explain non-compliances
C. The application of mechanisms that can reduce data protection risks
D. The implementation of a data protection policy

Question 37

What can help the controller to demonstrate compliance with the GDPR?

A. Adherence to an approved code of conduct
B. Maintenance of the records of processing activities
C. Implementation of data protection policies
D. All of the above

Question 38

Which body will monitor compliance with the approved codes of conduct?

A. A certification body accredited by the supervisory authority
B. The supervisory authority
C. The European Data Protection Board
D. The Data Protection Officer

Question 39

What is included in the supervisory authority's powers?

A. Impose a temporary limitation on the processing
B. Impose a definitive limitation on the processing
C. Order the suspension of data flows
D. All of the above

Question 40

What may be the worst consequence of an infringement of the processing principles?

A. A fine of up to €10m or 2% of the total worldwide annual turnover
B. A fine of up to €20m or 4% of the total worldwide annual turnover
C. A prison sentence
D. A bankruptcy order

Answers

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

How to book your exam?

All our exams are delivered through an online examination system called ProctorU. To enrol for an exam, go to: https://www.seco-institute.org/certification-exams/how-to-book-exam/

Make sure you are well-prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

Review the examination rules at

https://www.seco-institute.org/html/filesystem/storeFolder/10/Rules-and-Regulations-for-SECO-Institute-Examinations-2017-11.pdf

Digital badges

SECO-Institute and digital badge provider Acclaim have partnered to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

SECO-Institute doesn't issue certification titles for Foundation courses. However, upon successful completion of your Foundation exam, you can claim your digital badge free of charge at the SECO-Institute.

https://www.seco-institute.org/claim-your-foundation-badge

PDPF-Sample Exam-EN-v2.0