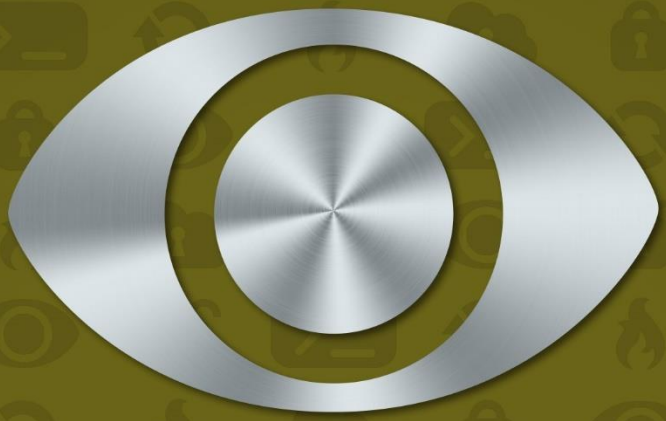

PRIVACY & DATA PROTECTION

PRACTITIONER

Sample Exam Questions

SECO INSTITUTE

Introduction

This document contains 4 questions (and answers) that help you familiarise yourself with the structure and topic areas of the SECO-Institute's Privacy & Data Protection Practitioner certification exam.

To download our Complete Sample Exam, create a free study account at https://members.seco-institute.org

We recommend you to take the Complete Sample Exam before registering for the certification exam.

The results of the Sample Exam do not count towards your examination score.

Certification exam

You can book your exam through one of our accredited training partners or directly with the SECO-Institute. To book an exam through the SECO-Institute, go to https://www.seco-institute.org/how-to-book-your-exam-schedule-an-exam/

By passing the certification exam, you demonstrate that you possess the knowledge and skills necessary to transition to a data protection role. You can perform a Data Protection Officer's most important tasks from raising data protection awareness to interfacing with data subjects, and you can advise your management on achieving and maintaining GDPR-compliance.

Exam format

- Computer-based with remote proctoring
- Multiple-choice questions and essay-type questions
    - 10 multiple-choice questions
    - 5 short open-ended questions
    - 1 essay question based on a case study
- Time allowed: 120 minutes
- Closed-book exam
- Pass mark: 65%

Questions

Question 1

The GDPR requires controllers to perform a Data Protection Impact Assessment (DPIA) where the processing "is likely to result in a high risk to the rights and freedoms of natural persons". As a DPO, which activity would you subject to a DPIA in any event?

A. HR and recruitment
B. Access rights management
C. Supplier relationship management
D. Accounting and bookkeeping

Question 2

Bicsma's marketing department uses a popular online marketing platform to create newsletter campaigns. The platform is operated by a U.S.-based service provider. As Bicsma's DPO, you need to advise Bicsma on how to use the platform and remain GDPR-compliant. What will you do?

A. Verify whether the provider has joined the EU-U.S. Privacy Shield framework. If the answer is yes, the issue requires no further action from Bicsma. The Privacy Shield framework has obtained an adequacy decision from the European Commission, and personal data transfers under an adequacy decision are regarded as intra-EEA transfers.
B. Inform the relevant stakeholders that the platform should not be used until Bicsma and the provider sign a legally binding agreement.
C. Check whether the provider has a representative in the EU. If there is an EU-representative, GDPR-compliance is automatically ensured.
D. Read the provider's data protection policy. If the policy states that the provider will process personal data in accordance with the GDPR, it is safe to use the service.

Question 3

Which of the following statements is correct?

A. 'Risk appetite' refers to the amount of risk an organisation needs to take in order to achieve its strategic objectives.
B. 'Risk capacity' refers to the amount of risk an organisation needs to take in order to achieve its strategic objectives.
C. 'Risk tolerance' refers to the amount of risk an organisation can afford to take.
D. 'Risk appetite' refers to the amount of risk an organisation can afford to take.

Question 4

As Bicsma's DPO, you realise that My Can of Bicsma's Privacy Notice is very basic. It only describes what categories of personal data Bicsma collects from its customers, and how Bicsma uses that data to deliver orders, answer inquiries and send newsletters.

List 4 more content elements you would include in the Privacy Notice.

Answers

Question 1

The correct answer is A. HR and recruitment should be subjected to a Data Protection Impact Assessment in any event.

The Article 29 Working Party's *Guidelines on Data Protection Impact Assessment* list 9 criteria the controller should consider when determining the level of risk inherent in the processing. The general rule is that the more criteria the processing meets, the more likely it is to present a high risk to data subjects, and therefore to require a DPIA. The Working Party strongly recommends controllers to perform a DPIA if the processing meets at least 2 out of the 9 criteria listed below (form Module 2, Section: DPIA in the Context of the GDPR):

1. Evaluation or scoring, including profiling
2. Automated decision-making that has a significant effect on the data subject's rights and interests
3. Systematic monitoring
4. Sensitive data (special categories of personal data, such as health data)
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects (power imbalance between the data subject and the controller)
8. Innovative use (new technological or organisational solutions)
9. The processing prevents data subjects from exercising a right or using a service or a contract

HR and recruitment meet at least 3 criteria: 2, 4 and 7:

2. Recruitment is likely to use automated decision-making that may have a significant effect on the data subject.
4. Sensitive data are processed (a typical example is the processing of health data for sick leave management purposes).
7. HR processing concerns vulnerable data subjects (employees). Vulnerable data subjects are those who may be unable to oppose the processing due to an increased power imbalance between the data subject and the controller.

Considering that HR and recruitment is likely to meet at least 3 of the 9 criteria, a DPO should recommend the performance of a DPIA on this process in any event. Naturally, this does not mean that a DPIA cannot be (or should never be) performed on access rights management, supplier relationship management, or accounting and bookkeeping. Those processes may also use personal data, but whether or not they require a DPIA depends on the particular circumstances.

Module 2 – Impact and Risk Assessment, Section: DPIA in the Context of the GDPR

Question 2

The correct answer is B. Inform the relevant stakeholders that the platform should not be used until Bicsma and the provider sign a legally binding agreement.

The GDPR requires controllers to conclude binding agreements with all their processors. It is true that the U.S. has obtained an adequacy decision, the scope of which is limited to those U.S. organisations that comply with the Privacy Shield. It is also true that the GDPR regards personal data transfers under an adequacy decision as intra-EEA transfers. Yet the controller's obligation to conclude legally binding agreements with its processors applies to all controller-processor relationships. The GDPR contains no specifications on the binding agreement: it may be drawn up either by the processor or the controller, and it may be a standard document which the controller accepts when accepting the terms of use. The only important point is that the agreement must be binding and must address all the requirements set out in Article 28 of the GDPR.

The GDPR mandates that non-EU controllers and processors who process the personal data of individuals who are in the EU appoint a representative in the EU. Yet responsibilities for compliance with the GDPR cannot be transferred to the representative and having a representative is no guarantee for a controller's or processor's GDPR-compliance. Similarly, a processor's data protection policy does not guarantee that the processor will process personal data in line with the GDPR.

Module 3 – Operations, Section: Contract Management: Data Processing Agreements

Question 3

The correct answer is A. 'Risk appetite' refers to the amount of risk an organisation needs to take in order to achieve its strategic objectives.

The three correct statements are:

- Risk appetite refers to the amount of risk an organisation needs to take in order to achieve its strategic objectives.
- Risk tolerance refers to the amount of risk an organisation prefers to take.
- Risk capacity refers to the amount of risk an organisation can afford to take.

Module 2 – Impact and Risk Assessment, Section: Risk Management

Question 4

Correct answers may include:

- A description of the data subject's rights
- An overview of how data subjects can submit requests and complaints
- The contact details of Bicsma's DPO
- The (categories of) recipients of the personal data
- Whether or not the personal data will be transferred to an entity outside the EU/EEA (if yes, reference to adequacy decision or safeguards)
- A description of the technical and organisational security measures
- The data retention periods per processing purpose/personal data category

Module 1 – Strategic Considerations, Section: Privacy Notice