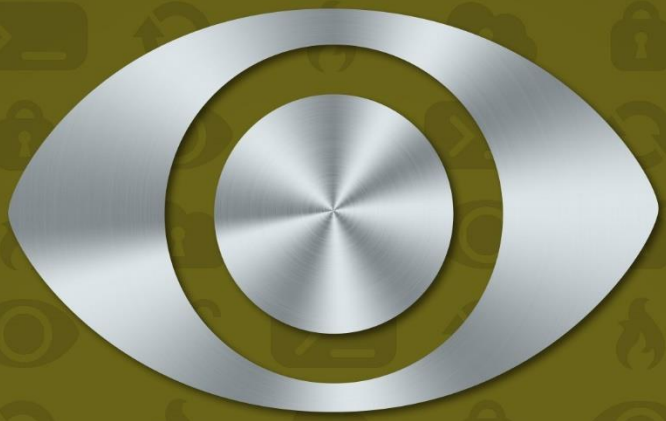

PRIVACY & DATA PROTECTION

PRACTITIONER

Sample Exam

SECO INSTITUTE

General information

The SECO-Institute issues its official Cyber Security & Governance courseware to 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 Practitioner exam (with a passing score of 60%), candidates receive a Privacy and Data Protection Practitioner certificate and a digital badge.

This Sample Exam allows candidates to familiarise themselves with the structure and topic areas of the current Privacy & Data Protection Practitioner certification exam. 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 candidate's examination score.

Examination details

- Computer-based
- Multiple choice questions and essay-type questions
    - 10 multiple choice questions: 3 points per question
    - 5 open-ended questions: 8 points per question
    - 1 essay question based on a case study: 30 points
- Time allotted for examination: 120 minutes
- Pass mark: 60% (60 points out of 100 points)
- Open book/notes: not permitted
- Electronic equipment: not permitted

Rules to be observed by candidates

The SECO-Institute's Examination Rules and Regulations: https://www.seco-institute.org/html/filesystem/storeFolder/10/General-Terms-and-Conditions-for-participation-in-SECO-Institute-exams-2017-11.pdf

Note

This sample exam contains 5 multiple choice questions, 3 open-ended questions, and 1 essay question.

The certification assessment contains 10 multiple choice questions, 5 short open-ended questions and 1 essay question.

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

Due to a web application vulnerability, an EU-based video game website leaks the usernames and passwords of 700 individuals in a readable format. The games on the website do not feature loot boxes or any valuable items. As the company's DPO, you need to decide who must be notified of the breach. Who will you inform and why?

A. The competent supervisory authority. You cannot demonstrate that the breach is unlikely to result in any risk to the data subjects whose login data have been leaked, therefore you must notify the supervisory authority. The data subjects need not be notified. According to the GDPR, the data subjects must be notified only if the risk is high, and high risk is a subjective notion. You can reasonably assume that a third party gaining access to usernames and passwords that are only used to play free games, does not represent a high risk to the data subjects.

B. The data subjects. Although you believe that the risk to the data subjects is moderate, you know that the data subjects have the right to know what has happened to their personal data. The supervisory authority needs not be informed, as the personal data breach does not involve sensitive data and only concerns a relatively small number of individuals.

C. The competent supervisory authority and the data subjects concerned. The supervisory authority must be notified, as you cannot show that the breach will not result in any risk to the data subjects. The data subjects must be informed, because this breach is likely to result in a high risk to them, even though it does not involve sensitive data.

D. Nobody needs to be informed. The breach concerns a small number of individuals and only involves login data used on a video game website. It is very unlikely that those data could be used in such a way that it would result in any risk to the data subjects. You are confident that the supervisory authority will accept your argumentation, should an investigation be initiated.

Question 3

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 4

Privacy by design is an approach that seeks to embed privacy considerations into the design and operation of systems, networks and business practices. Which is one of the seven foundational principles of privacy by design?

A. Privacy as the default setting
B. Zero sum over positive sum
C. Security at the data level
D. Compartmented information facilities

Question 5

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 6

You are Bicsma's new DPO, just starting your job. You need to conduct a gap analysis to determine Bicsma's current data protection posture and to identify actions needed to ensure Bicsma's compliance with the GDPR.

List 5 main areas you will address in your gap analysis.

Question 7

List 6 topics that must be addressed in a GPDR-compliant data processing agreement.

Question 8

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.

Question 9

Complaints procedure for Bicsma

As Bicsma's DPO, you realise that Bicsma has no formal procedure for handling data subject complaints. List the steps that should be included in Bicsma's complaints procedure.

Answers

Question 1

The correct answer is A. HR and recruitment.

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 C. The competent supervisory authority and the data subjects concerned.

The GDPR states that the supervisory authority must be notified of all data breaches, unless the breach is unlikely to result in a risk to the rights and interests of natural persons. Naturally, if the controller decides not to notify the supervisory authority, it must be able to support its decision with good arguments. In practice, this means that the controller should be able to demonstrate to the supervisory authority that the breach is unlikely to result in a risk to the data subjects (for example, by referring to the security measures taken). If the controller cannot demonstrate that the breach is unlikely to result in any risk, the DPO should recommend that the supervisory authority be notified.

The GDPR requires the controller to notify the data subjects if the breach is likely to result in a high risk to the rights and freedoms of natural persons. The severity of the breach is determined based on the number of the data subjects concerned, the nature of the personal data involved in the breach, and several other factors. Although login data on a game website are not sensitive data, a good DPO would assume that many data subjects use the same usernames and passwords on other websites, such as government or online banking websites. The risk should be regarded as "high", and thus the data subjects should also be notified.

Module 3 – Operations, Section: Data Breach Procedure

Question 3

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 4

The correct answer is A. Privacy as the default setting.

The principle of "privacy as the default setting" states that personal data should be automatically protected in any IT system or business practice. The maximum degree of privacy should be provided automatically, without requiring any action from the data subject.

The other six principles are:

- Proactive not reactive; preventative not remedial
- Privacy embedded into design
- Full functionality; positive-sum not zero-sum
- End-to-end security; full lifecycle protection
- Visibility and transparency
- Respect for user privacy

Module 4 – Design and Implementation, Section: Privacy by Design/Default

Question 5

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 6

Correct answers include:

- Note existence/lack of a strategic data protection policy. If a policy exists, assess policy content and employees' knowledge about, and understanding of, the policy.
- Compliance with the processing principles.
- Data subject rights management: request and complaints procedures.
- Security of the processing.
- Data protection impact assessments.
- Processing registers and personal data breach documentation.
- Personal data breach notification procedure
- Applicability of requirements relating to personal data transfers outside the EEA.
- Level of data protection awareness: trainings and workshops held, effectiveness of awareness activities…

Module 5 – Governance, Section: Data Protection Management System

Question 7

Correct answers include:

- The processor is only allowed to process personal data on the controller's documented instructions (unless the processing is necessary to comply with an obligation under Union or Member State law).
- The processor provides the controller with all the information necessary to demonstrate compliance with the GDPR.
- The processor imposes confidentiality obligations on its personnel.
- The processor ensures the security of the personal data by implementing appropriate technical and organisational measures.
- The processor only engages other processors (sub-processors) if expressly authorised by the controller.
- The processor imposes the data protection requirements set out in the processing agreement on any sub-processors.
- The processor assists the controller in facilitating the exercise of data subject rights.
- The processor assists the controller in ensuring compliance with the controller's data breach notification obligations.

Module 3 – Operations, Section: Data Processing Agreement (DPA)

Question 8

Correct answers include:

- A description of the data subject's rights
- An overview of how data subject requests and complaints can be made
- 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)
- The data retention periods

Module 1 – Strategic Considerations, Section: Privacy Notice

Question 9

The most crucial elements are:

- Receive the complaint (designate first point of contact).
- Assess the validity of the complaint. If you decide to refuse the complaint, inform the data subject of the decision and explain why you are refusing the complaint.
- Register and label/classify the complaint.
- Assign the complaint to the responsible party. Inform the data subject that you have accepted the complaint and transferred it to the relevant party. Indicate when the data subject should expect to receive a reply.
- Process the complaint and keep the data subject up to date. If you realise that processing the complaint would take longer than one month, inform the data subject of the delay and explain why extra time is needed.
- There may be a standard routine for handling certain categories of complaints. If there is a DPO-approved routine, process the complaint accordingly. If you are not dealing with a standardised complaint, perform the necessary research and/or consult the DPO.
- Depending on the outcome of your consultation with the DPO, perform and document the actions needed.
- Notify the data subject of what you have done. Inform the data subject that the complaint will be closed, unless they object to you closing the complaint.
- Close the complaint and assess your way of handling the complaint. Assessing your effectiveness will enable you to improve the process and standardise recurring complaints. Standardisation, in turn, may allow you to have less experienced staff members deal with the complaints, or maybe even automate the process.
- If the data subject disagrees with closing the complaint and underpins their view with acceptable arguments, try to resolve the complaint in a different way.
- If the data subject disagrees with closing the complaint but fails to provide valid arguments, ask the data subject to explain why they are objecting to closing the complaint. If the data subject still fails to provide relevant arguments, inform them that you will close the complaint.
- If the data subject still disagrees with closing the complaint, refer them to the DPO.
- If the data subject remains dissatisfied, refer them to the DPA.
- Keep a record of all (internal and external) actions and communications related to the complaint. This enables you to demonstrate that you were acting in good faith, should a complainant decide to take their complaint to the DPA.

Module 3 – Operations, Section: Complaints Procedure

Workbook – Elaboration of Case Study 4 (Complaints Procedure)

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://go.proctoru.com/

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

If you are a new user, select Test Taker. Select "SECO-Institute" as the institution and fill in all the necessary information. See the instructions for more information. Once you have scheduled your exam, you will be asked to pay the exam fee. If you have an exam voucher, please fill in the access code.

Our online examination system allows you to book and take your exam at your convenience. It is up to you to decide where and when you will be tested.

System requirements

To ensure the quality and security of the examination, you will have to meet specific requirements regarding your computer configuration, your exam environment and your behaviour during the exam. Click here to see the requirements.

The exam will be taken with special proctor software. To enable webcam and audio recording during the exam, you have to install software that monitors your activities.

Your exam will be recorded through your webcam and microphone. After you have completed the exam, the recordings will be checked by multiple proctors to see whether you comply with all the requirements.

Results

If no non-conformities are detected by the proctors, you will receive the final result by email one month after completing the test. The email will contain information on how to claim your certificate and digital badge, and how to use your title.

Certification title

Upon successful completion of an exam, you can request your certification title from the SECO-Institute. To maintain a Practitioner certification, you need to earn and submit 20 Continuing Professional Education (CPE) credits yearly, a total of 60 credits over the three-year certification cycle. CPE requirements can be fulfilled by attending conferences, seminars, webinars or other trainings, through self-study, and through teaching activities and publications.

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/

Digital badge

The 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 enable certification holders to convey to employers, potential employers and other interested parties the skills they have acquired to earn and maintain a specialised certification.

Claim your title at: https://www.seco-institute.org/claim-your-title