

Re-Exam, Legal Aspects of Information Security

Your grade will be influenced by how well your answer is organized, on the micro-level as well as on the macro- level. Clarity is a virtue.

Where possible, state your sources. When referring to sources, you do not have to put down the full references, but they should be identifiable.

- Examples: “Article 6 of the GDPR”” Or “the *Smith v. Sweden* case from the European Court of Human Rights is an interesting example of...”

Time is scarce and **word count is limited to 2500**. It may be necessary for you to first try to identify the most pressing issues to be dealt with. For full credit on the question, it is not necessary that all issues are dealt with in detail.

The following grading scale is used:

- Fail (F, FX)(below 50 points)
- Sufficient (E)(50-59 points)
- Satisfactory (D)(60-69)
- Good (C)(70-79 points)
- Very Good (B)(80-89 points)
- Excellent (A)(90-100 points)

Students will be graded on the basis of facts, focus and form as follows:

- Facts - ability to demonstrate knowledge of the issue(s).
- Focus - ability to analyze the issue(s).
- Form - ability to present a well-structured and formulated answer.

You are not permitted to use any generative AI tools, including ChatGPT.

Question 1:

Chegg is a company established in Stockholm (Sweden) which markets and sells direct-to-student educational products and services. Its “Chegg Services” products and services include online learning aids, such as online tutoring, writing assistance, a math-problem solver, and answers to common textbook questions. Chegg has asserted that the target audience for its services is primarily university-level students.

In providing its services, Chegg collects personal information from users such as names, dates of birth, personal numbers numbers, and financial information. Furthermore, in connection with its online tutoring services, Chegg records videos of tutoring sessions that includes Chegg users’ images and voices.

As part of its information technology infrastructure, Chegg uses a third-party service provided by Amazon Web Services called the Simple Storage Service (“S3”). S3 is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The S3 stores data inside virtual containers, called “buckets,” against which

individual access controls can be applied. Chegg relies on S3 buckets to store a wide variety of files that contain users' personal information, including their names, passwords, dates of birth, and personal numbers.

Chegg permits employees and contractors to use a single access key that provides full administrative privileges over all data in the S3 databases. It stores users' and employees' personal information on Chegg's network and databases, including S3 databases, in plain text. It also uses outdated and unsecure cryptographic hash functions to protect users' passwords. They have no policies, processes, or procedures for inventorying and deleting users' and employees' personal information stored on Chegg's network after that information is no longer necessary for the purpose for which it was collected.

In or around September 2023, a Chegg employee fell for a phishing attack, giving the threat actor access to video recordings of tutoring sessions of thousands of students. Many of these videos contained the personal data of not just the tutors and students but also third parties such as family members captured in the recordings.

In or around October 2023, a former contractor accessed one of Chegg's S3 databases and exfiltrated a database containing personal information of approximately 40 million users of the Chegg platform. The exposed personal information included users' email addresses, first and last names, passwords, and, personal numbers.

In November 2023, a threat intelligence vendor informed Chegg that a file containing some of the exfiltrated information was available in an online forum.

Part 1A (25 points):

You work in the legal department at Chegg. Prepare a memo detailing the legal issues raised in this scenario and how you will respond, if at all.

Part 1B (25 points):

Hans is a history student at Stockholm University who purchased online tutoring services from Chegg in May 2023. In early December 2023, he was shocked to receive a notification from Anonymous Hacker that video recordings from his tutoring sessions at Chegg would be shared with his employer and family unless he paid a sum of 2000 EURO. In these recordings, Hans shared deeply personal information with his tutor, namely that he was a supporter of extreme right-wing political parties in Sweden, a topic that came up during their discussions of World War II.

Upset and aggrieved, Hans has turned to his local Data Protection Authority in Sweden, the Swedish Authority for Privacy Protection (IMY), seeking redress against Chegg. You work at IMY. Decide whether to impose fines and if so, on what basis.

Question 2 (25 points):

The concept of “Active and Assisted Living” (AAL) broadly refers to the use of innovative and advanced Information and Communication Technologies (ICT) to create supportive and inclusive applications and environments that may enable older, impaired, or frail people to live independently and stay active longer in society. An example of an AAL technology is a fall detection system.

Hana is an older adult who lives alone. Her son, John, who lives in a different part of the same city, has decided to provide her with a video monitoring technology called Fallo that sends him and her healthcare provider an alarm signal with an image if a fall occurs.

Explain how Fallo, the company developing and selling this technology can protect its intellectual property rights. Also consider whether Hana, the user of the AAL technology, has any intellectual property rights.

Question 3 (25 points):

Explain the relationship between the AI Act and the Cyber Resilience Act.