ZPRSGS

Anonymkod/Anonymous code: ZPRSGS

TENTAMEN/EXAMINATION

SECLAW HT2023

Rättsliga aspekter inom IT och info

Tentamen/Written exam 7,5 hp/hec

IB432C (SU) 432T AF

Poäng Points	Betyg Grade

Fredag/Friday 2024-02-23
08:00-12:00

Markera besvarade frågor med 'X' / Mark answered questions with 'X'													Antal blad # sheets
1	2	3	4	5	6	7	8	9	10	11	12		

Vakt kontrollerat antal blad:

Obs! Denna sida måste ligga överst - This page should be placed in front
Avlägsna tomma blad före inlämningen
Remove empty sheets before handing in the exam
Fyll i samtliga uppgifter på sidhuvudet på varje blad
Please fill in all information in the header on each sheet

[Assignment] Write your answers here

Answer to Question 1 part A:

Issue:

Chegg using third party s3 database has experienced multiple incidents of data breaches where unauthorized users gained access to personal data, including private videos of its users as well as the third parties filmed in the videos. Furthermore, Chegg is also lacking appropriate security measures for handling of sensitive personal data and users information around its networks and data centers.

Rule

The GDPR, particularly Article 32(security of processing) in combination with article 33 (informing authority) , article 34 informing the subject and Article 5 (Principles relating to processing of personal data), outlines the requirements for protecting personal data and ensuring the confidentiality, integrity and availability of processing systems.

Analysis:

Lack of adequate security measures:

Chegg lacks adequate security measures, allowing unauthorised access to personal data, violating Article 32 of the GDPR.

Data Breach Impact:

The data breach is affecting a large number of people including students,staff their relatives and third parties which is the violation of the principles of data processing outlined in Article 5 of GDPR.

Responsibility:

Chegg company as the main controller of the data is responsible for ensuring the security and integrity of the personal data processed by the third party acting as processor.

Chegg is also responsible to inform the authority about the breach of data and the affected people.

Chegg is also responsible to immediately take corrective measures in order to ensure no such breaches in future.

Conclusion:

Chegg fails to comply with the article 32 (security of processing) of GDPR by not implementing appropriate technical and organizational measures to ensure the security of the personal data.

Chegg also fails to comply with the article 5 (principles relating to processing of personal data) of GDPR as inadequate security measures resulted in unauthorised access to personal data, violating the principles of data processing.

Chegg is exposed to imposition of heavy fines and penalties due to leak of personal data and the fines depends upon the severity of the breach, the corrective measures and the duration of the breach which in chegg case is a very severe as big data is being leaked to unauthorised persons.

Answer to Question 1 part B:

Issue:

The Chegg company failed in protecting the personal data of Hans student at stockholm university who is under ransomware attack by hacker. Because of lack of security measures at Chegg company Hans very personal data got into hands of unauthorised person and now Hans wants legal action against Chegg.

Rule:
Several GDPR (General Data Protection Regulation) articles are relevant to this case:

- Article 5, this article guides on the principles of lawfulness, fairness, and transparency in data processing. It requires that personal data be processed for specific purposes and not exposed to unauthorised access by third parties.
- Article 32, dealing with the security of processing, in this context Chegg is obliged to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. In this case the leak of personal data indicates a lapse in data security measures.
- Article 33, deals with notification of personal data breach to the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Article 34, communication of a personal data breach to the person or the data subject.

Analysis:

Chegg failed to uphold the principles of data processing, implement adequate security measures, and fulfill notification obligation both to the supervisory authority and the

affected individual.

Conclusion:

Imposing fines on Chegg is justified based on violations of GDPR articles related to data processing principles, security measures, and breach notification requirements.

Answer to Question 2:

Issue:

How can Fallo company protect intellectual property. Hana user of such technology intellectual rights available or not.

Rule:

Directive 2001/29/EC of the European Parliament

Analysis:
In order to recognize and secure intellectual property rights in an AAL technology is a very critical task for a developer. Patent would protect the functionality of the AAL technology used by Fallo. However it is a very difficult task to get patent approved for AI tools at the moment but instead they can be protected as trade secrets under the relevant regulations. There is also benefit in trade secrets instead of patent as trade secrets normally do not need to be applied and filed to relevant authorities which makes them complaint of the legal requirements of relevant region and can get automatic protection. But it has very low rights as compared to the patents. So in my view individual assessments are necessary for some parts Fallo should get patents and for some parts trade secrets.

Conclusion
Fallo can get intellectual rights under laws for the videos and audios but at the same time user Hanna can also argue for the personal data collected in such process as a customer or user of such technology of Fallo.

Answer to Question 3:
Relationship between AI act and Cyber Resilience Act:

In order to protect the rights of citizens the European Commission is taking many initiatives and one of the key initiative in this respect is the AI act and Cyber Resilience Act. EU commission has formulated draft regulations for AI products i.e. AI Act that will deals with regulating the high risk AI products. In complement to the AI act ,the Cyber Resilience Act (CRA) acts as a horizontal regulations that will regulate the market of software and hardware products having digital elements.
There is a very common interconnected relationship between CRA and AI act because of the nature of the products as of technology i.e. security of the products being in market for sale is the basic requirements in order to protect the fundamental rights, democracy, rule of law and environmental sustainability . For simplicity, we can say

that CRA provides the baseline cyber security requirements for such connected devices. In a nutshell the AI systems that are considered to be at a higher risk of causing harm will comply with the relevant AI Act as well as must follow the essential requirements listed in Cyber Resilience Act as well. The relationship further extends to demonstrate through EU declaration of conformity of complying with such acts.