Exam, Legal Aspects of Information Security

The following standards apply regarding your answers for the questions:

- 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. 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.
- 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.
- Please note that it is *not* possible to upload a PDF. This is because of the automatic word limitation.
- Write your anonymous code on your exam (*not* your name).

Question 1 (40 points):

Founded in 2011 and established in Stockholm (Sweden), Whiz is a videoconferencing platform provider that furnishes customers with videoconferencing services and various add-on services, such as cloud storage. Whiz's core product is the Whiz "Meeting," which is a platform for one-on-one and group videoconferences. Whiz Meetings also have the capability, among other things, for accompanying chat messages, screen sharing, and the recording of videoconferences.

Whiz routinely collects certain information about users, including: first and last name; email address; user name and password; approximate location; date of birth; technical information about users' devices, network, and internet connection; and in the case of a paid subscription, billing address and payment card information of the account holder. Whiz also collects and stores event details for all Whiz Meetings, including the date, time, and length of Meetings; the Meeting participants' user names; and each participant's answers to any polling questions asked during a Meeting. Finally, Whiz also collects and stores information shared while using the service, such as recorded Meetings that users store on Whiz's cloud storage, voice mails, chat and instant messages, files, and whiteboards.

Whiz offers customers the ability to record their Whiz Meetings and store such recordings on either the host's local device or, for paying customers, in Whiz's secure cloud storage ("Cloud Recordings"). In Whiz's Security Guide, Whiz states that Cloud Recordings are processed and stored in Whiz's cloud "after the meeting has ended," where they "are stored encrypted as well." Even though Whiz claims that Cloud Recordings are processed and securely stored in Whiz's cloud once the meeting has ended, in fact, recorded Meetings are kept on Whiz's servers for up to 60 days, unencrypted, before Whiz transfers the recordings to its secure cloud storage, where they are then stored encrypted.

In May 2022, Hans, a resident of Sweden and a paying customer of Whiz Meetings, attended an online therapy session with an expert located in New York via Whiz which was recorded. During this session, Hans revealed highly sensitive information about his life including information about his sexuality, mental well-being, and physical well-being including information about an HIV diagnosis.

In April 2022, Hans, who not yet revealed to his parents that he was HIV positive, was shocked to receive a notification from Anonymous Hacker that his personal data would be shared with his employer and family unless he paid a sum of 2000 EURO.

Feeling outraged, victimized, and violated, Hans turned to his local Data Protection Authority in Sweden, Swedish Authority for Privacy Protection (IMY), seeking redress against Whiz. You work at IMY. Decide whether to impose fines and if so, on what basis.

Question 2 (20 points):

Discuss the relationship between the information security requirements found in the GDPR and the AI Act, if any.

Question 3 (20 points):

Digital signatures are more secure than handwritten signatures. Argue in favor or against this position from both legal and technical perspectives.

Question 4 (20 points):

AI raises many intellectual property issues. Discuss the relationship between AI and intellectual property with regard to (A) AI and copyright and (B) AI and patents.

Öppnades: måndag, 13 februari 2023, 09:00
Senaste inlämningsdatum: onsdag, 15 februari 2023, 09:00

The exam consists of several short-essay style questions. Students will have 24 hours to complete the exam at home and a limit of 2000 words.

Question 1

In this answer, I assume that the Anonymous Hacker accessed the information through Whiz's unencrypted servers and not from the expert in New York who could potentially have saved the meeting on his/hers local device unencrypted and then got hacked.

Fines would be imposed for three reasons: the recordings of the meetings that are stored on Whiz's cloud storage service "Cloud Recordings" are left unencrypted for up to 60 days on Whiz's servers; the disinclination to notify the authorities about the breach; and disinclination to communicate to the data subject about the breach.

In GDPR Article 2 (1): "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system". Since the processing of personal data occurs on cloud, video, chat, servers etcetera, therefore GDPR is applicable.

In GDPR Article 4 (1): "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly". Since it's not specified in GDPR any format for the information, one could argue that the recordings of the meetings are considered personal data. In this case with Hans, the recordings certainly included personal data: his face; voice; username; mental status etcetera. With all this information, Hans could be both directly and indirectly identified.

In GDPR Article 5 (1.e): "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ". Whiz has for an unnecessarily long period kept the personal data of the data subjects in a form which permits identification of data subjects when the recordings of meetings are stored unencrypted on their servers for up to two months before being transferred to the cloud storage.

In GDPR Article 9 (1): "Processing of personal data revealing [...] data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited ". Whiz could not know that Hans would tell the expert during their therapy session about his sexuality, well-being etcetera, Hans has given his permission to process this data, he has not given permission that his sensitive personal data is stored unencrypted on Whiz's servers.

In GDPR Article 32 (1): "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". Since Whiz already has the appropriate technical measures, to some extent, to ensure that their customers' personal data is secure (storing it encrypted on their cloud storage service), but they also lack technical and organisational measures to ensure that the personal data is secure before it's transferred from their servers to their cloud storage service.

In GDPR Article 33 (1): "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours". Since Hans is the one to notify authorities about the breach and not Whiz (within the 72 hour deadline) The company has also not had any obvious reasons to think that the data breach would unlikely result in a risk to their customers. In this case, the breach resulted in a violation against Hans' rights and freedom.

In GDPR Article 34 (1): "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay". It must have been known by Whiz that the customers' recordings are left unencrypted on Whiz's servers for up to two months before transferring the data to the cloud storage.

In GDPR Article 83 (1): "Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive".

In GDPR Article 83 (4): "Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher [...] a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43" In this case, Whiz has violated article 32 (1), 33 (1) and 34 (1).

In GDPR Article 83 (2): "Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points a) to h) and j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; b) the intentional or negligent character of the infringement; c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; g) the categories of personal data affected by the infringement". In this case we do not know if the character of the infringement was intentional or negligent, but we do know that Hans has suffered great damage and Whiz has not taken any action to mitigate this damage that Hans has suffered.

Question 2

GDPR and the AI Act have the same legal base which is TFEU Article 16 which protects individuals personal data. To some extent, this would mean that the AI Act would complement GDPR in protection afforded to data subjects.

The AI Act Article 9 regulates risk management systems and GDPR Article 22 can provide useful criteria that providers should consider when conducting risk analysis.

In GDPR Article 33 (1): "...not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay".

In the AI Act (5.1): "AI providers will be obliged to inform national competent authorities about serious incidents or malfunctioning that constitute a breach of fundamental rights obligations as soon as they become aware of them, as well as any recalls or withdrawals of AI systems from the market. National competent authorities will then investigate the incidents/or malfunctioning, collect all the necessary information and regularly transmit it to the Commission with adequate metadata. The Commission will complement this information on the incidents by a comprehensive analysis of the overall market for AI".

In both GDPR and the AI Act, controllers/AI providers are obliged to report incidents/breaches to national competent authorities. In GDPR Article 33 (1), controllers shall notify the personal data breach if the data breach is likely to result in a risk to the rights and freedoms of natural persons, and in the AI Act (5.1), AI providers will be obliged to inform national competent authorities about serious incidents/malfunctioning that constitute a breach of fundamental rights obligations. Three significant differences between the two are:

1) controllers have 72 hours after having become aware of a personal data breach to notify authorities, whereas AI providers will be obliged to inform authorities about serious incidents/malfunctioning as soon as they become aware of them;

2) where the notification to authorities is not made within 72 hours, controllers shall state reasons for the delay, AI providers will not have any mitigating circumstances for delays on informing authorities;

3) AI providers will have to recall/withdraw AI systems from the market in case of a serious incident/malfunctioning, whereas controllers do not have to withdraw any systems from the market in case of a personal data breach.

Question 3

Just like physically signing a contract, digitally signing consists of the same building blocks: signer, authentication to prove identity of signer and the document to be signed. Both processes start the same by creating a document. Instead of authenticating the signer by, for example, a drivers licence, the signer authenticates them by entering a code or biometrics to the signature creation device. Instead of signing a paper with ink, the signer uses their private key to sign the contract.

Qualified electronic signatures have, in the whole EU, the equivalent legal effect of a handwritten note (ENISA, Security guidelines on the appropriate use of qualified electronic signatures, 2016). By using a qualified trust service provider (QTSP) to sign a document, users are provided with better legal protection. For example, if an incident regarding the signature occurs that would result in litigation between party A and party B, the burden of proof would lie on the QTSP.

From a technical perspective, it's also easier to collect data regarding the signing of a document compared to handwritten signatures in order to prove or dismiss a claim in a litigation between two parties. For example:

- A drivers licence can be forged and if there's no photocopies of it, it's hard to prove, while a ton of data is created when a signer authenticates themselves by entering, for example, a code: device-, network-, position data etcetera is collected. If the code is used on a new device in an area where the signer is not located, it strengthens the claim of forgery.
- A person's handwritten signature can differ over time, whereas an authenticating code plus the signer's private key equals clear format.
- A handwritten signature can be difficult to tie to a specific location since it does not contain any such inherent capabilities, whereas it's fairly difficult to forge where a digital signature occurred.

Question 4

AI systems can create new content that could fall under copyright laws, such as visual art and texts. According to WIPO, creative works qualify for copyright protection if they are original and in most jurisdictions, only works created by a human fall under the protection of copyright. If an AI creates new creative works using other people's copyrighted material, it is not an infringement of their copyright given that the end result is original enough. In theory, this could mean that companies investing in AI systems for creating new content could be left without any payment from users since the content is not protected by law and anyone in the world is allowed to use it for free.

Computer-implemented inventions are treated differently depending on the patent office's region in the world. One can apply for a patent on national level, European level and worldwide (Sweden, EPO and WIPO). EPO has guidelines for examination of the patent requirements, which are: novelty; inventive step and susceptibility of industrial application. The same approach applies to computer-implemented inventions related to AI. As long as the invention fulfils the patent requirements, a patent can be granted and valid in Europe.

Tillbaka

◄ SEC LAW reexam 30 JAN 2023

Hoppa till...