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.

Question 1 (25 points):

Flo&Co, a company located in Stockholm (Sweden), pitched its Flo Period and Ovulation Tracker as a way for women to "take full control of their health." Flo&Co's app allowed users to log their menstruation days in a handy period calendar, track their ovulation and fertility, schedule menstrual cycle reminders, record moods and PMS symptoms, use a due date calculator, and follow a pregnancy calendar. In its privacy policy, Flo&Co stated that it would only use individual's personal data "to provide services in connection with the App."

After using the app for 1 year, Elsa discovered she was pregnant. This was an unintended pregnancy and Elsa felt deeply confused about how to handle it. Nevertheless, she entered this pregnancy-related information into the app so she could track her progress while she contemplated how to manage the situation. Because the so-called "App Event" contained the word "pregnancy" in the title, it was automatically disclosed to a third-party marketing and analytics firm called Beta, a major technology firm headquartered in California, United States. Furthermore, the personal data that was sent to Beta was in an unencrypted format allowing it to be intercepted by a malicious actor who threatened Elsa to reveal to her family and employer that she was pregnant unless she paid 1500 Euro.

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

Question 2 (55 points):

Travel Med is a company located in Stockholm, Sweden which sells a wide array of emergency travel membership plans that cover up to fifteen different emergency travel and medical evacuation services for members who sustain serious illnesses or injuries during travel in certain geographic areas. These services include, for example, hospital-to-hospital air transportation, vehicle return, visitor transportation, repatriation for recuperation near home, medical escort flights, and transportation of children. Membership plans provide coverage on a short-term, yearly, or multi-year basis for both single members and entire families. Depending on the term, number of members, and the medical evacuation services covered, membership plans cost between 2000 SEK and 10,000 SEK.

Consumers purchase membership plans through an online application on Travel Med's website. Through this application, Travel Med collects a significant amount of personal information from applicants, including name, date of birth, sex, home address, email address, phone number, emergency contact information, passport number, and payment card information. It also collects detailed health information such as a list of prescribed medications and medical conditions, as well as all hospitalizations in the previous six months. Consumers cannot purchase membership plans without providing Travel Med with this information.

Part (a) (15 points):

In March 2021, Marcus, a dual Swedish-American citizen, and a resident of Stockholm, decided to travel to New York for a 6 month stay. Because the Swedish Foreign Ministry advised against travelling to America during the pandemic and therefore his home insurance would not cover any accidents/health-related costs, he decided to get some extra insurance from Travel Med. Travel Med required that the contract be signed electronically with a qualified electronic signature using a program called DocuBind. What key properties does such a signature provide, particularly from the perspective of legal and security properties?

Hundreds of thousands of consumers have signed up for Travel Med's membership plans, meaning it has collected a large amount of personal information about these consumers. Travel Med has made a significant investment to build a commercial database to utilize these data. Not only has it spent large sums of money to develop a suitable structure for the database so that the desired data may be efficiently accessed but it has also invested heavily in storage of all of the data.

Part (b) (20 points): You work at Travel Med. Prepare a memo exploring whether Travel Med is able to exploit this data from the perspective of intellectual property.

In March 2022, a security researcher, using a publicly available search engine, discovered a separate and unsecured cloud database maintained by Travel Med. According to the security researcher, the database, which could be located and accessed by anyone on the internet, contained approximately 100,000 membership records with individuals' information stored in plain text, including information populated in certain fields for names, dates of birth, gender, home addresses, email addresses, phone numbers, membership information and account numbers, and health information (i.e., "hospitalized," "prescription," and "medical").

Part (c)(20 points): You work at Travel Med. Prepare a memo exploring how to respond to this notification. Make sure to address legal compliance concerns from the perspective of Travel Med as well as the individual's whose data is handled by Travel Med.

Question 3 (20 points):

Discuss the relationship between AI, data protection and information security, if any.

Öppnades: tisdag, 10 januari 2023, 12:00
Senaste inlämningsdatum: onsdag, 11 januari 2023, 12:00

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

Issue: *Whether there was a personal data breach?*

Rule: If there is a data breach that is likely to result in a high risk to the rights and freedoms of the data subject, Flo&Co needs to notify the personal data breach the supervisory authority (DPA) according to Article 33 GDPR and the data subject according to Article 34 GDPR. If there is a personal data breach, fines are imposed on Flo&Co according to Article 83 GDPR.

Analysis: According to the territorial scope of Article 3(1) GDPR, the regulation applies to any controller established in the European Union (EU). Based on Article 4(7) GDPR, Flo&Co is the controller since it determines the purposes (providing services in connection with the app) and the means (data merging and storing etcetra).

Flo&Co is processing special categories of data (sensitive data). It includes, for instance, data concerning health or sex life (Article 9(1) GDPR). Fo&Co is processing sensitive data regarding pregnancy-related information such as menstruation, fertility, and moods. The main rule is that Flo&Co is not allowed to process this data. However, there are exemptions. For example, if the data subject gives her explicit consent to the purpose of the processing (Article 9(2)(a) GDPR). The consent must be freely given, specific, informed, and unambiguous (Article 7 GDPR). In this case, I assume that Elsa has given her explicit consent to the defined purpose by an active behavior. However, Elsa still has a right to respect for private life (Article 8 ECHR/Article 7 CFR).

Article 5(1)(b) GDPR states that personal data shall be collected for a specified, explicit, and legitimate purpose and not further processed in an incompatible manner (purpose limitation). Flo&Co needs to specify a lawfully stated reason to the data subject as to why they are processing personal data. In this case, Elsa's data was disclosed to a third-party firm and then processed by a new controller (Beta) for a new purpose (analyze and market her) – without her consent and knowledge. Therefore, this violates purpose limitation and the fairness principle of Article 5(1)(a) GDPR since the controller is not transparent about the processing.

Moreover, Flo&Co sent Elsa's personal data to Beta unencrypted. Article 32 GDPR states that the controller and processor shall implement appropriate technical and organizational measures for confidentiality and integrity to ensure an appropriate level of security to the risk by considering state-of-the-art and costs of implementation. Article 32(1)(a) GDPR explicitly mentions encryption as one possible measure. This control could assure a security level appropriate to the risks to Elsa's freedoms and rights, which Fo&Co should have demonstrated by building security mechanisms into their system under privacy by design and default (Article 25 GDPR).

Conclusion: The more sensitive data, the higher the data security should be. Since Fo&Co processes sensitive data, it must meet stricter requirements of Article 32. Even though the amount and type of data could be proportionate to the app's purpose, the data was unencrypted, resulting in a breach. Fo&Co also breaches Article 25 in the failure to have built into mechanisms to prevent the breach in the first place. As a controller, Fo&Co needs to assess the risk to the freedoms and rights of the data subject. In this case, the breach resulted in a high risk to Elsa's rights and freedoms since she was blackmailed into revealing information about her private life. Based on Article 33 GDPR, Fo&Co needs to notify the DPA about the breach and Elsa based on Article 34 GDPR. IMY imposes fines according to Article 83 GDPR. Since Fo&Co did not deploy safeguards such as encryption, IMY is not considering any mitigation factors. Fo&Co is subject to fines of four percent of the undertaking's worldwide annual turnover or 20 million euros, whichever is higher.

Question 2(a)

Issue: *What key legal and security properties does a qualified electronic signature provide?*

Rule: Since TravelMed operates in the EU, the eIDAS Regulation is enforced. *eID* means a cross-border recognition for electronic identification and *AS* refers to trust services for electronic identification on the internal EU market (Determann, 2021). Article 25 eIDAS states that a Qualified Electronic Signature (QES) should have the same legal effect as a handwritten signature.

Analysis: A QES is the most advanced electronic signature. It is cryptographically based and uses a signature-based ID and a qualified signature-based creation device (QSCD), with a qualified certificate for electronic signatures, including hardware

protection for the key (Determann, 2021). QES ensures that the signature was created by the person claiming to have signed the document (non-repudiation). Anyone who receives the signed document can verify the signature based on the certificate. A QES is also unique and specific to the person signing the document. It also ties the signature to the document so that any alteration to the document can be detected (integrity).

Conclusion: It is difficult for someone to forge or alter a digital signature without detecting and making it invalid, which assures a high level of security. A QES can serve as evidence in court and is enforceable in the same manner as a physical signature (Article 25 eIDAS) in a jurisdiction that recognizes electronic signatures as legally binding.

Question 2(b)

Issue: *Whether TravelMed can exploit the data in the database from the perspective of intellectual property (IP)?*

Rule: The way that a database is constituted (selection and arrangement) can be protected by copyright as a collection or compilation (Article 2(5) Berne Convention/Article 10(2) TRIPS/ Article 5 WCT). Also, database protection on the EU level by Directive 96/9.

Analysis: TravelMed's database structure can be protected by copyright under Article 2(5) Berne Convention/Article 10(2) TRIPS/ Article 5 WCT. It can also have protection under Article 1(2) Directive 96/9 if it is an independent order of data. Article 3 states that it can get protection for the selection and arrangement of the data. However, the database's content could have individual protection, for example, copyright. Rightsholders have the exclusive right to use or authorize others to use or reproduce copies of the copyrighted work (WIPO Handbook, 2004).

If the database, for instance, includes pictures of the customers to demonstrate their injuries, which could be protected by their copyright, with other rightsholders (not TravelMed), if they meet the copyright requirements of, for instance, originality. This means that the rightsholders of those pictures could be their customers – and if the pictures can lead to a natural person being identified or identifiable, there are also data protection rights according to Article 4 GDPR. However, if TravelMed cuts the link between data protection rights, copyright, and pictures, it would be possible to exploit the data. For example, if the pictures are anonymized (GDPR is not applied), or if the database includes synthetic media or adversarial examples where the data looks like the data subjects, but machines will not recognize it due to minor changes in the pictures. In this way, an AI classificatory system can be tricked into misclassifying something (Bellovin et al., 2019).

Conclusion: Copyright law provides exclusivity – artificial protection to an intangible (the database). TravelMed could obtain copyright and/or database protection for the database's structure. The database can include other rightsholders' copyright-protected work, which TravelMed cannot use. However, suppose the database contains synthetic material, the link to data protection law and copyright law could be cut and data anonymized. In that case, it does not fall under the GDPR. If TravelMed can create a synthetic database, it could suddenly exploit it freely – if this would be ethical or not would be another question.

Question 2(c)

Issue: *Whether TravelMed had built-in appropriate security measures in processing personal data?*

Rule: Article 25(1) GDPR states privacy by design and default, namely that the controller must implement appropriate technical and organizational measures, for example, pseudonymization, to implement core principles such as data minimization.

Analysis: Based on Article 4 GDPR, TravelMed is on the hook for all the responsibilities of the GDPR since the data was not anonymized. Article 25(2) states that security controls should, by default, ensure that personal data is not accessible to an indefinite number of natural persons. TravelMed needed to build appropriate controls into their system beforehand, such as encryption (Article 32(1)(a) GDPR) or pseudonymization (Article 25 GDPR) and organizational measures such as information classification. Data also needs to be adequate, relevant, and limited concerning the purpose for processing – data minimization (Article 5(1)(c). Based on the circumstances, it is also questionable if the data was kept in a form that does not allow the identification of data subjects longer than needed for the processing purpose – storage limitation (Article 5(1)(e) GDPR). Identifiers were stored in plain text, and it is also questionable whether the amount of data is proportionate for the purpose. TravelMed did not restrict access to data by the lack of security measures which also violates the core principle of integrity and confidentiality in Article 5(1)(f) GDPR. New insight can be derived from these data points using AI, which could give rise to additional sensitive data points about the data subject's health or well-being. Then the general rule of Article 9 GDPR is that TravelMed is not allowed to process it.

Conclusion: Since TravelMed breached the core principles of Article 5, the court or the DPA may likely find the company of breaching Article 25 (privacy by design) in their failure to have built into mechanisms to prevent the leak in the first place. Since appropriate security measures were not implemented, Article 32 is also violated. This serious matter poses a significant risk to the customers' privacy and the company's legal and regulatory compliance. Immediate action is needed to address the data leak and mitigate the potential harm. The database should be shut down, further access limited, and further security controls such as encryption should be implemented to prevent similar incidents. Since the data leak poses a high risk to the data subjects' rights

and freedoms, TravelMed needs to notify the DPA based on Article 33 GDPR and the data subjects according to Article 34 GDPR.

Question 3

There is a relationship between Artificial Intelligence (AI), data protection, and information security, as they are intertwined and can impact each other. AI relies on data to learn and make predictions (Bellovin et al., 2019). On the one hand, AI could entail several advantages for data protection and information security. For AI to be effective, it should have access to vast amounts of high-quality data. Security terms such as integrity and availability are essential for developing and deploying AI. If the data is accurate – the AI itself will produce accurate results. AI could also enhance security by detecting and preventing cyberattacks. AI could be trained to identify patterns of malicious activity and respond to them in real time. AI could also automate many security tasks, such as vulnerability scanning, log analysis, and intrusion detection. Based on data protection, it might also be possible for AI to collect/ analyze personal data, which would result in minimal risk based on the proposed AI Act.

On the other hand, AI poses threats to data protection and information security. AI could reveal sensitive and confidential data points about individuals, as exemplified in question 2(c) above. In addition, AI can also bypass security controls and steal or manipulate data. Synthetic AI-generated media can also mislead humans (Veale & Borgesius, 2021). For example, fake news or voice fakes mislead people into specific behavior such as the transfer of money. A synthetic database could also impact the data quality. The AI Act could prevent humans from being misled by synthetic media in the EU. Unacceptable categories of AI systems will include social scoring (ibid.), which could pose data protection issues. Synthetic media can also mislead other AI systems through Generative Adversarial Networks and adversarial examples (Bellovin et al., 2019). This is a security risk, as seen with Tesla's self-driving cars, where an image of an altered traffic sign is put over a real traffic sign that confuses the self-driving Tesla car. Thus, it is essential to ensure that the AI system is robust to prevent malicious use and attacks.

Tillbaka

◄ SEC LAW exam 1 Jan 2022 final

Hoppa till...