RGZSDM

Anonymkod/Anonymous code: RGZSDM

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

Tisdag/Tuesday 2024-01-09
08:00-12:00

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

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

Question 1

Part 1A

This memo will highlight the legal issues that we at Boomin are facing because of the recent security incident. I understand that it can hard to understand the root cause of the issues, but they will be bright up here.

We at Boomin has developed new and innovative features but have not followed the GDPR. First of all, our new feature “Friends” are using biometric data which is classified as sensitive data according to article 9 of the GDPR. The basic standpoint of sensitive data is that is not advised to be used, but if you are, you need to get explicit consent from the data subject, according to article 9(2)(a). We have not done this since the feature was enabled by default. Building upon the argument invalid consent, article 9(2)(a) states that explicit consent can be given to a specified purpose. The important words here are explicit and specified, the consent was neither explicitly given and the purpose was not specified, and therefore not a lawful ground for processing. Furthermore, because the feature was enabled by default and there was no option to turn it off, we did not comply with article 25(2). Article 25(2) states that we as a controller, needs to ensure that technical and organisational measures are in place to ensure no processing takes place on personal data unless it is necessary. In this case it would be to not have it on as default. Further, the article also states that security measures ensuring that human interaction is needed to enable them. In this case it would be to have the ability to turn it on or off. The “Friends” feature also had the function of tagging people, which could also be a breach of article 9 of the GDPR. This is because a picture together with a tag with a name of the person could be linked to an individual, and are therefore personal data. This means that we are processing personal data of individuals other than our consumers, and therefore have no consent.

Another pressing legal issue is the lack of security for both the data as well as our systems. Our policy is stating that we will keep the data for a certain period of time, for example for legal issues. This is completely fine according to article 17(3)(e) of the GDPR, however, the data needs to be deleted when it is no longer necessary, which it has not done. Furthermore, our cybersecurity measures have not met the requirements of article 25(1) and article 32(1) of the GDPR. Such measures could be pseudonymisation, such as encryption, proper logging of security events as well as vulnerability testing.

We need to respond to this incident, since it is our obligation to report this to supervisory authority within 72 hours, according to article 33(1) of the GDPR.

Part 1B

There are multiple grounds for imposing fines upon Boomin for not being compliant with GDPR on multiple occasions, such as Article(5)(e), no lawful grounds for processing according to article 6, no grounds for processing of sensitive personal data according to article 9, and not achieving the security requirements on multiple parts of article 25 and 32. Article 79(1) states that, data subject has the right to judicial remedy against a controller if they a breach has occurred with regards to the GDPR and article 77(1) states that the data subject has the right to complain to a supervisory authority, which Hans has done to IMY.

If we look at article 82(2) of the GDPR, a couple of considerations are mentioned to be taken into account when choosing whether to impose fines or not. Article 83(2)(a) is stating that the severity of the infringement should be taken into account, such as the number of affected people. This case is of high severity since it concerns all consumers of Boomin when it comes to the infringement upon article 9 (no consent) and article 25 and 32. However, some individuals, such as Hans, have a stronger complaint because their data got leaked and article 82(1) is stating that data subjects have right to compensation if they have “...suffered material or non-material damage as a result of the infringement...”. Hans has in this case been blackmailed, which is material damage, but also non-material damage since all his photos are leaked. Therefore, fines as well as compensation to Hans and others are possible. Another consideration to take into account is 83(2)(d), if the controller or processor has taken their responsibility and implemented to required measures according to article 25 and article 32. This has not been done and another reason for fines. However, there are some considerations that can reduce the fines, for example 83(2)(c) and 83(2)(e). 83(2)(c) says that if the controller has tried to mitigate the damage, that should take into consideration, and 83(2)(e) states that if no previous infringements has been done, that should be taken into consideration.

However, because of the severity and widespread of the incident among Boomins consumers, fines should be given. According to article 83(5)(a), if either article 5, 6 ,7, or 9 has been infringed, fines up to 20 000 000 EUR or 4% of the annual turnover should be given. Fines for infringe upon article 25 or 32 is mentioned in 83(4)(a), however, you go with the most severe infringement.

Question 2

Part 2A

There are a number of strategies Cyber Innovation can use when protecting its products and services. Intellectual property rights ensures the holder of the IP to have exclusive rights of the usage, distribution and display of the thing covered by the IP. The first strategy is to choose what type of intellectual property it should go for, the

different types have different protection but also different costs and difficulty to achieve. The first category of consideration is patents, which can be inventions in the technical field, however it requires the innovation to have new findings or characteristics that previously was not known. When it comes to Cyber Innovation they have a innovative way of monitoring networks, but the idea itself does not contribute to anything new but rather building upon existing knowledge to put together a new way of using those features. The next Intellectual property of interest is copyright, which is often used for computer programs. Copyrights cover original artistic works, and it needs to be the authors own creation. Copyrights give the holder rights over distribution, production, and communication. This fits right into Cyber Innovations need for Standpoint. Copyrights also have less requirements and are easier to acquire than patents. Directive on Copyright in the digital single market 2019/790 is the regulation in use for copyright. One last intellectual property that might be useful for Cyber Innovation is trade secrets. Trade secrets rights will make it possible for Cyber Innovation to take legal remedies against someone who breaches a confidentiality agreement. It comes with some requirements, for example that secrecy of a method, process or formula will give Cyber Innovations a competitive edge and that the secret is not publicly known already. This can be very beneficial for startups if they have anything that make them have a competitive edge, for Cyber Innovations case it could be algorithms. Trade secrets are also less costly and easier to obtain. A combination of copyright and trade secret would be beneficial for Cyber Innovation.

Other important considerations to take into account before applying for intellectual property are your current obligations to other companies. In some cases people at a startup have different jobs because it is not profitable enough to get competitive salaries. In this instance it is important that the person applying for the IP, does not have any obligation to its current employer. Most organizations have a clause in employee contracts that all competitive innovations of the organization that are made by an employee belong to the employer.

The most important part of IP strategy is to acquire the appropriate IPR within a reasonable amount of time, to both minimize cost but also ensuring as fast as possible the right to ownership before anyone else does it.

Part 2B

The main regulation for electronic signatures in the EU is eIDAS, which promotes the usage of electronic signatures across the EU. E-signature is a secure way to remotely sign documents, and can be divided into three levels. Simple electronic signatures is the most basic electronic signature has no real tie to an individual or legal standpoint, it could for example be email signature. Advanced Electronic Signatures (AES) is the second level, and requires more security features, and they are tied to a specific individual and therefore is the individual identifiable. AES is usually done by an e-identification, such as BankID in sweden. Another security features is that it is using electronic signature creation data that a signatory has under his/her control. AES uses public key infrastructure to share encryption keys. The last level of e-signature is Qualified Electronic Signature (QES) and it has the same requirements as AES, it does however require a Qualified signature creation device, which is a physical device. QES is not widely used in Sweden and therefore might not be useable in some situations.

eIDAS article 25(1) states that an electronic signature that does not qualify as a qualified electronic signature should not be dismissed only on for that reason.

However, article 25(2) of eIDAS says that a qualified electronic signature has the same legal basis as a handwritten signature, and therefore a better choice from a legal standpoint. An AES, for example BankID, can be used an e-signature and identification solution for Happykey, since it is achieving trust level 3 of eIDAS and is inspected by the EU with regards to eIDAS. Because of this, from a legal standpoint, you can sign contract and invoices with this solution. However, from a legal standpoint QES is better within in the EU, but signing contracts such as employee contracts would be near impossible since the general public does not use it in Sweden. There are solution for QES that could work business to business and could work internationally, but limitations still exist within Sweden. Public authorities in Sweden allow BankID (which is an AES) to be used to sign government documents such as taxes. Most use cases for e-signature for Happykey can be achieved by AES and will have a strong legal standpoint within Sweden, however, internationally it might not be enough.

Question 3

The fast development of AI and its increasing use does come with significant security concerns as well as legal difficulties. Deep fakes falls under the category of limited risk and it therefore comes with transparency obligations, such as it should be disclosed if an image, audio or video has been manipulated. It can be disclosed with labels and/or watermarks. But, it does not necessarily mean that the user of deep fakes will disclose that, and therefore it should be automatically done by open and paid deep fake softwares. Furthermore, should AI systems include additional metadata stating that it is in fact AI generated, in case if additional modifications of a deep fake. This metadata can be used by automated systems to further disclose deep fakes, this can be especially important in propaganda campaigns in social media networks which concerns national security. This forces cybercriminals to build their own AIs. That is of course possible, especially with the amount of open source AI models. Here is where the AI act can fall short in some specific use cases, because the AI act does regulate AI systems as a whole and not certain components such as models. The AI act will however set requirements for security (article 15) and privacy. This should make it harder for criminals to use public AI systems for malicious use.

In todays digital landscape and the technological possibilities of ordinary persons, voice recognition should not have been used as an authentication option. Banks should use a physical device to login into, such as BankID on a phone or bank verification device. These passwords should only be able to change the password of those in person at the bank. From a data protection standpoint, a lot of information of a person is displayed online, in this case personal number and bank account was acquired, and it was probably from other attacks that then sold the information. Cyber Resilience Act (CRA) will put more pressure on products with digital elements to ensure a secure environment and therefore possibly limit the amount of data that is leaked and then can be used for even more malicious activities. Additionally, there needs to be a stronger enforcement of the GDPR to ensure data protection, it is a possibility that places where the data has previously been leaked didn't follow the appropriate security standards, to ensure both privacy and security measures, such as pseudonymization. This shows that the whole supply chain needs to be secure to ensure a widespread cyber resilience, which CRA aims to promote. It should also be a more robust detection mechanism for cybercrime activities, from a security

standpoint, the bank should check for location of the logins as well as additional verification for transfers to unusual places. However, the law has a hard time keeping up with technological development and therefore a lot of security problems that could be enforced with law, are not.