Seminar questions

1.

The CCO of GlobEl is concerned about its customer service department's level of performance a) To what extent – if at all – is GlobEl allowed to monitor employee emails for quality assurance? Would it be worthwhile to further specify the purpose of such a control measure? b) If the company decides to, for example, store the employee emails must they encrypt these emails?

Answers:

a)

GDPR permits workplace monitoring but not at the free discretion of the company. There are clear rules for when monitoring of emails is allowed and under what circumstances.

Emails can be considered as private communication, and as such they meet the requirements of personal data as described in GDPR article 4, which states that personal data is any information that relates to a directly or indirectly identified or identifiable living natural person. Monitoring personal data, i.e processing of personal data, must according to article 5 be processed fairly and lawfully.

According to article 6 (1), which categorizes lawful processing of personal data, the only applicable points out of 6 possible are points (a) and (f). According to (a), the data subject has given consent to the processing of his or her personal data for one or more specific purposes. This comes at odds with the fourth point in article 7, which states that in the case of consent being given, it must be given freely, and among other things, that it is given under the condition that there is no imbalance of power between the two parties. The workplace relationship between an employer and employee is in direct violation of this article and as such, the only use case here would be the one described in point (f), which states: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject". Therefore, the company has the right to monitor employee emails due to legitimate interests. These interests however must be specified. I personally find the term quality assurance vague, and I believe that it would be viewed with suspicion if GlobEl was obliged to present their legitimate interests in a court or other legal setting.

Thus, my final conclusion is that it is in the interest of GlobEl to further specify the purpose of the control measure in order to strengthen their claim to legitimate interest. That is, they have the right to monitor employee emails, but must present a more specific and legitimate reason for doing so if they are ever put on the spot.

b)

Article 5 of the GDPR lists the principles of data protection you must adhere to, including the adoption of appropriate technical measures to secure data. Encryption and pseudonymization are cited in the law as examples of technical measures you can use to minimize the potential damage in the event of a data breach. I interpret this as GlobEL having the obligation to ensure confidentiality of the personal data they store. How they wish to do this however is their choice entirely, as encryption is one of several ways to protect data.

Under Article 32, controllers are required to implement risk-based measures for protecting data security. One such measure is the “pseudonymization and encryption of personal data”

In conclusion, encryption of personal data is not mandatory and GlobEl does not have to do it, but it is the most common and preferred way of ensuring confidentiality.

2.

A data controller must be aware of the different users who access their systems/records and their requirements. The CCO is wondering how GlobEl manages the rights of access to the various types of data (i.e. personal data, sensitive data, general business data etc.) within the organization? Are there any legal requirements to provide customers with access to their data?

Answer:
According to article 15 of GDPR, Right of access by the data subject, companies are required to provide subjects with information regarding their data. This includes but is not limited to: the purpose of processing, copies of the personal data undergoing processing (first time free of charge, subsequent issues can be requested for a fee) and the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.

3.

GlobEL’s operations are complex, and collaboration is critical to innovation and service delivery. “The world has changed,” says an information security service area leader at the company. “We need tools to create a secure environment, but we also need to facilitate collaboration, growth, and the appropriate relationships that drive business forward.”

Given that the transmission of personal data and other sensitive information is critical to GlobEl’s business, especially the transfer of data to third countries such as the United States, the CCO wonders what strategies should be applied?

Answer:
To start off, according to the previously mentioned article 15, data subjects have the right to be informed whether personal data is transferred to a third country or international organization.

According to article 45, Transfers on the basis of an adequacy decision, transfers of data are allowed and do not require specific authorisation as long as the country in question ensures an adequate level of protection of said data. This adequacy can be broken down into three main components, the prevailing strength of the countries rule of law, the efficiency of its regulatory and supervisory bodies regarding compliance with data protection rules, and finally, how much the country in question abides by legally binding conventions regarding data protection. Those countries that are deemed secure are determined by a special European GDPR commission. The USA is not considered to be a country that implements enough safeguards.

If the country in question does not fulfill the requirements mentioned in article 45, then the guidelines of article 46, Transfers subject to appropriate safeguards, must be followed. In the absence of or inadequate implementation of safeguards, the transfer of personal data is allowed if and only if the controller has ensured that the data in question is sufficiently protected according to the conventions in article 45. If this cannot be ensured, data transfer is not allowed.

In conclusion, data transfer to countries not considered safe is considered to be allowed as long as the controller or GlobEl takes the steps necessary to ensure that the data is protected. As such, if data is transferred to a party within a country considered unsafe, the CCO should make sure to sign legally binding contracts that explicitly state that the data will be protected in accordance with GDPR rules.

4.

In general terms, cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. How can GlobEl Sweden move to the cloud with confidence, particularly where it is clear that EU data protection law places the responsibility for data security squarely on the data controller who is accountable to the individual data subject for the safeguarding of their personal information? In other words, how can GlobEl Sweden be satisfied that data will be secure if it is outsourced to a cloud provider?

Answer:

Assuming that the data is transferred to within Sweden, the question clearly states that the data controller is ultimately responsible for the data in question. Thus, upon choosing a cloud service provider, they must ensure that the provider acts as if beholden to the same GDPR standards as is the controller. When the processor and controller is not the same entity, the controller must choose the processor in adherence with GDPR article 28, which among other

things states that the processor must give legally binding guarantees that the data of all affected subjects is protected and handled in accordance with GDPR. Additionally, the processor is not in turn allowed to outsource the function of the processor without written authorisation from the controller and in which case this is allowed, the second hand processor must adhere to the same principles laid out in article 28.

In conclusion, the controller must pick out a processor that is compliant with GDPR, according to the points presented in article 28.

5.

The threat of insiders stealing valuable corporate data continues to escalate, particularly because it is difficult to detect and these people often have access to sensitive information. The inadvertent exposure of internal data has also become of critical concern. Such data leaks can expose enterprises of all types to serious regulatory, public-relations and financial risks. For example, Barclays Bank lost the sensitive data of 27,000 customers and, as a result, suffered devastating consequences to its reputation and received heavy fines as a penalty for this lapse in security. How can GlobEl protect itself against the risk of data loss? What kind of dataloss-preventive strategy(ies) should GlobEl utilize? Is there reason to base such a strategy on an information analysis and a data category classification? Are there any examples that could serve as an illustration?

Answer:

It is my belief that the CCO should operate under the assumption that their data at some point will be either lost or stolen. As such, precautions must be taken to ensure that data is protected even in those cases. That is, data must be encrypted and pseudoanonymized in order to ensure that the data is difficult to obtain in the case of it falling into the hands of a malicious adversary. According to article 4, “Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately”. Thus, pseudoanonymization coupled with sufficient organizational measures is a good way of making sure that unauthorized insiders do not have access to full records. Additionally, having the aforementioned additional information kept separately and or encrypted ensures that untrusted insiders cannot access it without private keys.

I could not answer the two last questions.

6.

John, a GlobEL employee, brought home his company laptop. Unfortunately, his home was broken into that very same day and the laptop was stolen. This incident resulted in the loss of 26.5 million company records. These records included, among other things, information about the names, dates of birth, genders and personal numbers of employees and customers. What legal concerns are raised when employees use their own devices to access our company information? How could another event like this be protected against in the future?

Answer:

This implies that the data was physically stored on Johns laptop, which is unacceptable. I will therefore assume that the said amount records were uncovered and stolen, but that they still remain on company servers.

According to point (f) article 5, personal data must be processed in a manner that ensures appropriate security and protection against unauthorized or unlawful processing and against accidental loss. As such, it is unacceptable that data can be retrieved by a burglar simply by opening a laptop. This is in clear violation of article 5, as there are sufficient technical remedies that ensure the safety of data, be it strong passwords or encryption. Furthermore, two-factor authentication can be used, for instance as with Google Cloud Services, where access to records is impossible unless the authorized person has approved it.

As far as the use of personal devices is concerned, data processing must adhere to the same points and principles that have been discussed in the previous questions. There should be no legal concerns as long as data is treated in the same way it would be at company headquarters.

If the breach, regardless of if it happened on a personal or company device, poses 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, as per article 34, Communication of a personal data breach to the data subject.

7.

Considering the business conducted by GlobEL, which cybersecurity measures are the company compelled to take in order for it to be compliant with the law. In other words, which cybersecurity laws are applicable considering the business operations of the company and what demands do these legal rules place on the company?

Answer:

The core business of GlobEl belongs to the energy and utility sector. Depending on the size of and nature of the goods and services that GlobEl provides, they might be considered as Operators of Essential Services (OES) and as such they fall under the regulation presented in the NIS directive (Network and Information Systems). Some sectors, like energy

infrastructure and those of various financial institutions for instance, are considered to be critical for a functional society. The safety of these sectors is of great importance and are as such a matter of national security. Therefore they have their own set of corresponding regulations that overrule that of the GDPR wherever they overlap, and provides complementing guidelines where they do not. In broad terms, the NIS directive can be boiled down to following the following three main points:

- Securing networks and information systems by taking technical and organizational measures appropriate to the risk;
- Ensure service continuity by taking appropriate measures to prevent and minimize the impact of any incidents
- Notify regulators of any security incident that has a significant impact, less they want to face grave consequences of not doing so.

Many companies choose not to report security incidents and breaches in order to not lose business reputation and potential customers. One of the main points of the NIS directive is to discourage this. Non-compliance with the NIS directive is subject to heavy financial fines set by each individual EU member country.

This is an example of where special situations have warranted the introduction of additional directives, another instance of such being the EIDAS, which provides EU regulation on electronic identification and trust services for electronic transactions across the entire EU market.

8.

There have been widespread reports in the media that several hi-tech companies incorporated and whose headquarters are established in Sweden have been subject to an advanced persistent threat (APT) operation. Hundreds of terabytes of technical data about the companies' products and services, emails of the companies' employees, internal memos, and other documents have been exfiltrated. The goal of the operation appears to be to obtain trade secrets and other intellectual property from the companies' computers and networks.

At this stage, it is too early to be able to decisively identify who is behind the operation. However, there is preliminary evidence that the group behind the operation were acting on the instruction of a military intelligence unit of the Peoples' Republic of Nicha (PRN). Early investigations also indicate that at least one diplomat accredited to the PRN's embassy in Sweden and physically located in Sweden also took part in the operation under authorization from the PRN.

What breaches of international law are presented in this scenario? In your view, would PRN be responsible under international law for any of these breaches? What obligations under international law does Sweden have in responding to these incidents? What are the different legal options available to Sweden to address these incidents?

Answers:

Vienna Convention on Diplomatic Relations (VCDR) states among other things that it is the assignment of the diplomat to cultivate and promote friendly relations to the host country. What is essentially espionage is in direct conflict with the last statement. Thus I consider that such behavior is a violation of that agreement. The same convention states however that a diplomat cannot be held liable in court (diplomatic immunity). With regards to the diplomat, Sweden can only choose to expel them, what in colloquial terms is described as a unilateral decision to declare the diplomat to be a persona non grata.

According to the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual), the principle of non-intervention applies to war initiated or conducted through cyber-attacks (19). In the context of remote espionage through surveillance systems, the same rules on non-intervention, sovereign equality and political independence should continue to apply. The commentary to the Tallinn Manual states that cyberespionage operations lacking coercive elements do not per se violate the non-intervention principle. What they have done however is that they must certainly have committed illegal acts according to Swedish law. Sweden might thus be in a position to indict foreign internationals and require their extradition.