- mina egna tankar, funderingar
- citerar från uppgiften
- citerar från samarbeten
- citerar det jag själv hittat från nätet/skolmaterial-canvas

<u>QUESTION1</u>

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?

Short answer:
To the extent of "legitimate interest" (not "consent") within GDPR's limits.
It would be worthwhile as to make sure not to break against any GDPR's "*in a transparent manner*" and *burden of legitimate interest justification*.

Longer answer and brainstorming:

If "employee emails" consider the work emails of employees (A professional email address is the email address used for business communications, that is based on your custom domain. In other words, a professional email address is one that has your business name in it, in the form of a domain name) then xxx

If it considers personal email provided/not provided used for both bussiness/private affairs then xxx

Free consent could also be in doubt in situations of subordination

The validity of consent, which must have been freely given, as a legal basis for processing data about employees may be questionable, considering the economic imbalance between employer and employees. The circumstances surrounding consent must be assessed carefully

A common data protection problem in today's typical working environment is the extent of monitoring employees' electronic communications legitimately within the workplace. It is often claimed that this problem can easily be solved by prohibiting private use of communication facilities at work. Such a general prohibition could, however, be disproportionate and unrealistic. The ECtHR's judgments in Copland v. the United Kingdom and Bărbulescu v. Romania are of particular interest in this context.

Example: In Copland v. the United Kingdom,[931] the telephone, email and internet usage of a college employee was secretly monitored to ascertain whether she was making excessive use of college facilities for personal purposes. The ECtHR held that telephone calls from business premises were covered by the notions of private life and correspondence. Therefore, such calls and emails sent from work, as well as information derived from the monitoring of personal internet usage, were protected by Article 8 of the ECHR. In the applicant's case, no provisions existed which regulated the circumstances under which employers could monitor employees' use of telephone, email and the internet. Therefore, the interference was not in accordance with the law. The Court concluded that there had been a violation of Article 8 of the ECHR.

imbalances and subordination

under CoE law?

an employee's consent should be acknowledged as the legal basis for processing??? or the processing must be based on another lawful ground for processing???

According to the Article 29 Working Party, "[e]mployees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer."

By contrast, any operation involving the processing of personal data could fall under the scope of data protection rules and trigger the right to personal data protection. For example, where an employer records information relating to the names of and remuneration paid to employees, the mere recording of this information cannot be regarded as an interference with private life. Such an interference could, however, be argued if, for instance, the employer transferred the employees' personal information to third parties. Employers must in any case comply with data protection rules because recording employees' information constitutes data processing.

The directive also contains rules to ensure the accountability of controllers. They must designate a data protection officer to monitor compliance with the data protection rules, to inform and advise the entity and employees carrying out the processing of their obligations, and to cooperate with the supervisory authority.

Proportionality and procedural guarantees against arbitrariness were essential and the ECtHR identified a number of factors which were relevant in the circumstances. Such factors included, for example, the extent of the employer's monitoring of employees and the degree of intrusion into the employee's privacy, the consequences for the employee and whether adequate safeguards had been provided.

Processor VS Controller

Example: The Everready company specialises in data processing for the administration of human resource data for other companies. In this function, Everready is a processor. Where Everready processes the data of its own employees, however, it is the controller of data processing operations for the purpose of fulfilling its obligations as an employer.

(https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf)

"The parent company is established in Germany with wholly owned subsidiaries in the Nordics, South Africa and the USA."

Data of customers from Nordic is covered by GDPR laws, *regardless of where the data is processed*. Based on this, this could mean that sensitive customer data could need to be transferred outside of EU, depending on where the employee who will "monitor employee emails for quality assurance" works. If they work in South Africa or the USA, this done wrongly could break against the GDPR.

"*monitoring the behaviour of individuals in the EU*?"

Art. 84 GDPR Penalties - in case of violations - all member states must implement penalties for violating these rules.

*Personal data shall be processed lawfully, fairly and in a **transparent** manner in relation to the data subject.*

ART 5,6,7

consent or there is a legitimate interest; DIPA?

This tells me that they should absolutely inform both customers and employees subjected to any kind of recording/monitoring. And if anything changes from the original information presented to customers and employees they should be asked/informed anew.

energy company - *NIS directive*? operators of essential services (OES); and. relevant digital service providers (RDSPs)?

b) If the company decides to, for example, store the employee emails must they encrypt these emails?
Short answer:
Yes, it must?

Longer answer and brainstorming:
Article 32 section 1: the pseudonymisation and encryption and ***the ability to ensure the ongoing***

energy company - *NIS directive*? operators of essential services (OES); and. relevant digital service providers (RDSPs)?

The GDPR does not mandate specific technologies or implementations, so **no rule says, "you must encrypt personally identifiable data."** However, GDPR Article 32 (1) states that data controllers and processors must implement appropriate technological and organizational measures to secure personal data.

Email encryption is not required by GDPR, but it is considered to be an appropriate technical measure for protecting personal data.

appropriate safeguards such as the anonymisation, encryption or pseudonymisation of the data, and restriction of access to the data, must be put in place when further processing personal data.

https://www.nolo.com/legal-encyclopedia/email-monitoring-can-employer-read-30088.html??

an interference with private life. Such an interference could, however,
be argued if, for instance, the employer transferred the employees' personal information to third parties. Employers must in any case comply with data protection rules because recording employees' information constitutes data processing.

QUESTION2

How does GlobEl manage 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?

Every data subject has the right to information about any data controller's processing
of his or her personal data, subject to limited exemptions.
• Data subjects shall have the right to:
• access their own data and obtain certain information about the processing;
• have their data rectified by the controller processing their data, if the data are inaccurate;
• have the controller erase their data, as appropriate, if the controller is processing their data illegally;
• have the right to temporarily restrict processing;

Article 8 (2) of the EU Charter of Fundamental Rights, a document which constitutes primary EU law and has fundamental value in the EU legal order. EU secondary law – in particular the General Data Protection Regulation – has established a coherent legal framework which empowers data subjects by providing them with rights regarding data controllers. In addition to the rights of access and rectification, the GDPR recognises a series of other rights, such as the right to erasure ('right to be forgotten'), the right to object or to restrict data processing, and rights related to automated decision-making and profiling. Similar safeguards to enable data subjects to exercise effective control over their data are also included in Modernised Convention 108. Article 9 lists the rights that individuals should be able to exercise regarding the processing of their personal data. Contracting Parties must ensure that these rights are available to every data subject within their jurisdiction, and are accompanied by effective legal and practical means for enabling data subjects to exercise them.

Nature of the data

Any kind of information can be personal data provided that it relates to an identified or identifiable person.
Example: A supervisor's assessment of an employee's work performance, stored in the employee's personnel file, is personal data about the employee. This is the case even though it may just reflect, in part or whole, the superior's personal opinion, such as: "the employee is not dedicated to their work" – and not hard facts, such as: "the employee has been absent from work for five weeks during the last six months".
Personal data covers information pertaining to the private life of a person, which also includes professional activities, as well as information about his or her public life

Art. 15 GDPR

an interference with private life. Such an interference could, however, be argued if, for instance, the employer transferred the employees' personal information to third parties. Employers must in any case comply with data protection rules because recording employees' information constitutes data processing.

QUESTION3

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?

The law states that collected data should be limited to what is relevant and necessary for why they are collected in the first place. Therefore, corporations can only gather as much data about their workers as necessary and relevant for a given purpose. Also, the transfer of data collected on the EU 's citizens to a country outside EU is allowed under the following conditions: its jurisdiction ensures an adequate level of data protection, appropriate protection measures have been adopted or in special cases.

QUESTION4

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?

QUESTION5
QUESTION6
QUESTION7

QUESTION8

A state violates international law when it commits an "internationally wrongful act" - a breach of an international obligation that the state was bound by at the time when the act took place. A state is bound to act according to international treaties it signed.

Aspects:
Finally, peacetime espionage may also violate the Vienna Convention on Diplomatic Relations (VCDR) and the Vienna Convention on Consular Relations (VCCR). These conventions prohibit receiving States from committing espionage against the diplomatic and consular missions of sending States.[71] This legal framework imposes a triple lock of protection to this effect. https://ww3.lawschool.cornell.edu/research/ILJ/upload/Navarrete-Buchan-final.pdf

- Peacetime espionage
-
- Select 13 - Prohibition of intervention
-

- Cyber espionage per se , as distinct from the underlying acts that enable the espionage (see discussion in Rule 32), does not qualify as intervention because it lacks a coercive element. In the view of the International Group of Experts, this holds true even where intrusion into cyber infrastructure in order to conduct espionage requires the remote breaching of protective virtual barriers (e.g., the breaching of firewalls or the cracking of passwords).
-
-
-
-

Take the case of one State conducting cyber **espionage** against another. The latter finds out about the cyber **espionage** and summons the former's ambassador, **who then denies any cyber espionage. The situation qualifies as a dispute, but there is no obligation to try and resolve the matter because it does not endanger international peace and security.**

Rule 32 – Peacetime cyber **espionage** Although peacetime cyber **espionage** by States does not per se violate international law, the method by which it is carried out might do so. 1. This Rule applies only to cyber **espionage** conducted outside the context of an armed conflict. With respect to cyber **espionage** during armed conflict and the issue of spies, see Rule 89 . 2.

This Rule is limited to cyber **espionage** by or otherwise attributable to States (Rules 15 – 18). For activities conducted by non-State actors, see Rule 33 . Cyber **espionage** includes that which is directed at States, as well as commercial entities (e.g., so-called industrial **espionage** or economic **espionage**). The operations can target specific information or involve long-term bulk collection. 4. Cyber **espionage** can differ in both speed and volume from more traditional methods of **espionage**.

In particular, computer network exploitation is a pervasive tool of modern **espionage**. Though highly invasive, cyber **espionage** does not per se rise to the level of a use of force; indeed, there is no direct prohibition in international law on **espionage** (Rule 32). Thus, actions such as disabling cyber security mechanisms in order to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.

Select Part IV - The law of cyber armed conflict

- **Part IV - The law of cyber armed conflict**

This Rule is limited to cyber **espionage** conducted by members of the armed forces.

Select 16 - The law of armed conflict generally

Consider a situation in which units of the armed forces undertake cyber **espionage** directed at another State. The activity **does not in itself result in an armed conflict**, even if it is typically performed by civilian intelligence agencies, because the activity **does not satisfy the armed criterion.** 15.

https://www-cambridge-org.focus.lib.kth.se/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9/listing?q=espionage&searchWithinIds=E4FFD83EA790D7C4C3C28FC9CA2FB6C9&fts=yes&searchWithinIds=E4FFD83EA790D7C4C3C28FC9CA2FB6C9&aggs%5BproductTypes%5D%5Bfilters%5D=BOOK_PART

not so clear and no legal info
https://ww3.lawschool.cornell.edu/research/ILJ/upload/Navarrete-Buchan-final.pdf

- GDPR transfer of EU personal data outside

  The Experts noted that States frequently engage in cyber **espionage** (Rule 32), both within and beyond their territories. Although questions might arise as to the extraterritorial application of international 193 human rights law (Rule 34) with respect to **espionage**, the Experts were aware of no opinio juris suggesting that States consider **espionage** per se to fall beyond the bounds of their international human rights law obligations concerning the right to privacy.

- International Intellectual Property

https://www.rocketlawyer.com/business-and-contracts/intellectual-property/legal-guide/international-intellectual-property-law-101

While protecting your intellectual property (IP) rights in the United States is fairly straightforward due to the clear regulations concerning patents, trademarks and copyright, real problems start when you try to enforce your rights abroad. Countries may be signatories of international intellectual property protection agreements, each regulates the actual protection differently. To make matters worse, each type of intellectual property may be regulated differently.

While there is no common international copyright law, enforcement of copyright overseas is possible and even simple, as long as the target country is a signatory of the various international IP protection treaties, such as the Berne Convention or the TRIPS Agreement. Most signatory countries do not require registering copyrighted works, and confer protected status from the moment of creation. However, since everything ultimately depends on national regulations, you should always review the legal situation in the target country.

https://casebook.icrc.org/case-study/international-law-commission-articles-state-responsibility

CHAPTER I

INVOCATION OF THE RESPONSIBILITY OF A STATE

Article 42

Invocation of responsibility by an injured State

A State is entitled as an injured State to invoke the responsibility of another State if the obligation breached is owed to:

1. That State individually; or
2. A group of States including that State, or the international community as a whole, and the breach of the obligation:
    1. Specially affects that State; or
    2. Is of such a character as radically to change the position of all the other States to which the obligation is owed with respect to the further performance of the obligation.

Article 43

Notice of claim by an injured State

1. An injured State which invokes the responsibility of another State shall give notice of its claim to that State.
2. The injured State may specify in particular:
    1. The conduct that the responsible State should take in order to cease the wrongful act, if it is continuing;
    2. What form reparation should take in accordance with the provisions of part two.