The GDPR applies to:
a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed;
a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU.

GLOBAL VAR - Art. 84 GDPR Penalties - covers the penalties. If any of these rules are violated all member states must implement penalties for violating these rules.

Question 1

a)
ISSUE -
Does GlobEL have lawful ground to monitor employee emails?

RULES -
Because private communication falls under the definition of personal data defined in Article 4 of the GDPR the rules that apply here are.

- **Art. 5 GDPR Principles relating to processing of personal data** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Art. 6 GDPR Lawfulness of processing** - the data subject must give consent or there is a legitimate interest pursued by the controller.
- **Art. 7 GDPR Conditions for consent** - consent must be freely given.

ANALYSIS -
It will be difficult to get consent from the data subject and claim it was freely given considering that they may face a negative effect from not consenting. Therefore, the most appropriate ground will be legitimate interests. If the data subject disagree with your justification for legitimate interest the burden is on the controller to prove otherwise, therefore it is crucial that the benefits are obvious and that your reasons are thoroughly justified in documentation, because transparency of processing personal data between controller and subject is paramount.

If the employer has provided the email account then it is not considered a private email. However, if the emails consists of personal data, the above rules still apply. The employer must still make sure that all employees are made aware that their emails are being monitored.

CONCLUSION -
Yes, you can monitor employee emails, but you must be more specific than simply saying quality assurance. It would indeed be worthwhile to further specify the purpose of such a control measure.

b)
ISSUE -
Must GlobEL store employee emails in encrypted form?

RULES -
Because private communication falls under the definition of personal data defined in Article 4 of the GDPR the rules that apply here are. In addition the company is an energy company which means that it must obey the NIS directive.

- **Art. 32 GDPR Security of processing** - the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- **NIS Directive**

ANALYSIS -
They are required to protect personal data. Nonetheless encryption is not specifically required. We can reduce the probability of a data breach and thus reduce the risk of fines in the future if we encrypt personal data. In addition to GDPR, the NIS directive also specifies that the company must implement appropriate cyber security

CONCLUSION -
We are not obliged by the law to employ encryption, however I strongly advice that we do to reduce the risk of fines in the future.

Question 2

ISSUE -
Are there any legal requirements to provide customers or employees access to their data?

RULES -

- **Art. 15 GDPR Right of access by the data subject** The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.
- **Art. 9 GDPRProcessing of special categories of personal data**

ANALYSIS -
The data subject refers to both employee and customer. As such, both must be made aware what personal data is being processed, the purpose of the processing and have access to the personal data. When it comes to sensitive data/personal the employees must give explicit consent and there are rules on how this data shall be processed defined in Art.9, Art.5 and Art.32. GDPR only address personal data, not company data.

CONCLUSION -
Yes there are legal requirements when processing personal data, however, with regard to business data, it is up to GlobEL to deduce who in the company should be allowed access what data and implement access control policies.

Question 3

ISSUE - Are there lawful grounds for transferring personal data? And specifically to the United States?

What are the lawful grounds for transferring data to third countries?
RULES -

- **Art. 44 General principle for transfers** Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country must adhere to the provisions in Chapter 5 of the GDPR.
- **Art. 45 Transfers on the basis of an adequacy decision** If the third country does implement adequate safeguards.
- **Art. 46 Transfers subject to appropriate safeguards** If the third country does not implement adequate safeguards.

ANALYSIS -
Provided that there are lawful ground for the transfer itself in accordance with Art.6 and 9 of the GDPR, we must ensure that transfer to the third country is permitted. We must therefore differentiate between secure and insecure third countries. Secure third countries are those for which the European Commission has confirmed a suitable level of data protection on the basis of an adequacy decision and the United states is not part of that list. Therefore, we must ensure in another way that the personal data will be sufficiently protected by the

recipient in compliance with Art.46 (p.1). This can be done using standard contractual clauses.

CONCLUSION -
We can tranfer personal data to the USA if we first ensure that the personal data will be sufficiently protected.

Question 4

ISSUE -
how can GlobEl Sweden be satisfied that data will be secure if it is outsourced to a cloud provider?

RULES -
A cloud service provider will be considered a Data processor under GDPR, as such we must abide by the following rules:

- **Art. 5 GDPR** which defines the rules on how data shall be processed.
- **Art. 24 GDPR Responsibility of the controller** the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.
- **Art. 28 GDPR Processor** which defines the legal requirements between the controller and processor.
- **Art. 44 General principle for transfers** As when we do a data transfer to a third country we must adhere to the provisions in Chapter 5 of the GDPR.

ANALYSIS -
By Art. 24 Of the GDPR it is the responsibility of the controller to pick a processor that is adequate and compliant with rules regarding processing of personal data defined in Art. 5 of the GDPR. If the processor resides in a third-country, the controller must ensure that they implement adequate security measures for processing personal data which is stated in Art. 44 and all provisions in chapter 5 of the GDPR. In addition, we must ensure that the processor is compliant with the regulations defined in Art 28, on the relationship between controller and processor and the requirements of the processor itself.

CONCLUSION -
I advice we pick a cloud service provider that is GDPR-compliant to ensure that the processor operates on lawful grounds.

Question 5

ISSUE -
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?

RULES -

- **Art. 5 (1.f) GDPR** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- **Art. 25 GDPRData protection by design and by default** Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
- **Art. 32 GDPRSecurity of processing**

ANALYSIS -
————ART.32————
the pseudonymisation and encryption of personal data;

the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

How can GlobEl protect itself against the risk of data loss?
Implementing robust security measures to protect against unauthorized access to its data. This could include using strong passwords, implementing multi-factor authentication, and regularly updating and patching software to prevent

vulnerabilities.

Establishing clear policies and procedures for the handling of sensitive data, including policies on data access, data retention, and data disposal. Employees should be trained on these policies and regularly reminded of their importance.

Conducting regular audits and assessments of its data security practices to identify any potential vulnerabilities or areas for improvement. This could include conducting penetration testing, conducting regular backups, and implementing monitoring and detection systems to detect potential data breaches.

Implementing a robust data classification system to help categorize data based on its sensitivity and value. This could include classifying data as public, confidential, or sensitive, and implementing appropriate security measures for each category of data.

Is there reason to base such a strategy on an information analysis and a data category classification?
They should categorize data based on its importance and the more important it is the more security is required to have, since security must always be appropriate to the risk in accordance with Art.5 GDPR.

Are there any examples that could serve as an illustration?
AMAG Pharmaceuticals ran into a problem with data stored on Google Drive. A folder relating to HR activities was moved within the company's Drive, it stopped syncing properly. As a result, all the files seemed to disappear. After checking everywhere, including the trash bin and desktop, it seemed like the data was completely gone. Luckily the company was using a special tool specifically for the backup of Google drive files. They were able to restore all the files quickly and keep operations running smoothly.

Question 6

ISSUE - 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?

RULES -

- **Art. 5 (1.f) GDPR** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

- **Art. 32 GDPR Security of processing** - the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- **Art. 33 GDPR Notification of a personal data breach to the supervisory authority**

ANALYSIS -
Art.5.1.f) of the GDPR requires personal data to be: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). Additionally, article 32 specifies the obligations of the controllers to ensure the security, availability and confidentiality of the personal data, three goals data protection shares with information security.

It becomes apparent therefore, that for BOYD's benefits to be felt, companies must also implement security measures to safeguard their personal data assets.

The company must notify the supervisory authority of the data breach within 72 hours after having become aware of it.

CONCLUSION -
The employees may use their personal device but the company must ensure that the data being processed in accordance with Art.5 and 32. The ownership of the device does not matter only the data being processed.

Question 7

ISSUE - which cybersecurity laws are applicable considering the business operations of the company and what demands do these legal rules place on the company?

Because the company is an energy company and exists in european countries, it is regarded as critical infrastructure and must adhere to the NIS directive. The NIS directive takes precedence over GDPR where they overlap, but both are applicable. The NIS directive places demands on the cyber security of critical infrastructure. It is the responsibility of the member states to ensure that these rules are followed. Countries may have their own national laws on criticial infrastructe, for example in we have the PSA takes precedence over NIS and also places demands on the security of critical infrastructure.

Question 8

ISSUE -
What breaches of international law are presented in this scenario?

RULES -
With regards to the diplomat the applicable rules are:

- **Vienna Convention on Diplomatic Relations Art.41 (p.1)** Without prejudice to their privileges and immunities, it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State. They also have a duty not to interfere in the internal affairs of that State.

With regard to the military intelligence unit of PRN the applicable rules are:

- **Use of terror - AP I Art. 51 (2); AP II Art. 13 (additional protocol 1 and 2 to the geneva conventions)** may apply to cyber space. (IF REGARDED AS WARFARE)
- **UN CHARTER Art.2 (4)** All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

ANALYSIS -
The diplomat was in violation of Art. 41 of the Vienna Convention on Diplomatic Relations as they did not respect the laws of the receiving state.

Art.2 of the UN Charter has been violated since PRN did not respect the territorial integerity of the member state, sweden, as they conducted an illegal military opertation of foreign ground. This may also, if considered an act of warfare, be in violation of Additional Protocol to the geneva convention, Art 51 (2) and Art. 13 in AP 2 (Use of terror).

CONCLUSION -

ISSUE -
What obligations under international law does Sweden have in responding to these incidents?

RULES -

- **UN CHARTER Art.2 (3)** 3. All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.
- **Vienna Convention on Diplomatic Relations Art. 29** The person of a diplomatic agent shall be inviolable. He shall not be liable to any

form of arrest or detention. The receiving State shall treat him with due respect and shall take all appropriate steps to prevent any attack on his person, freedom or dignity.

- **GDPR Art.33 Notification of a personal data breach to the supervisory authority** 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

ANALYSIS -
In accordance with UN Chapter Art.2 (3) Sweden must act and settle this dispute by peaceful means. And accorind gthe Art.29 of the Vienna Convention on Diplomatic Relations, Sweden must ensure the protection his person, freedom and dignity.

In addition, company has an obligation to report the data breach under Art.33 of the GDPR.

CONCLUSION -

ISSUE -
What are the different legal options available to Sweden to address these incidents?

RULES -

- **Data breach is a crime according to chapter 4 section 9 c of the criminal code.**
- **Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning**

ANALYSIS -
Anyone who unlawfully prepares access to data that is intended for automatic processing or unlawfully changes, deletes, blocks or enters such data into a register is convicted of data breach.

the Swedish data-breach law provides compensates the GDPR resultion.

This data breach conducted by the PSR is in direct violation of Swedish data-breach laws. **CONCLUSION** -