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?

Yes, they are allowed if the email is under a company domain and used in combination with work. It would be worthwhile to further explain what the full extent of this monitoring would include and thereafter ask for permission. In cases where this is used is most likely that some sort of logging is required when a person is accessing emails to verify that the access is not being misused. In short if the company has legitimate interest in undertaking such a precaution. This needs to be in accordance with DIPA however.

b) If the company decides to, for example, store the   
employee emails must they encrypt these emails?

Yes, because this conversation could be a private one between two persons. It is not posted anywhere and therefore the data sent between these members should be encrypted. Article 32 section 1

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

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?

As few people as possible should have the right to view this data in accordance with Article 5 section 1

1. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

Article 15 section 1 specifies that a subject should have right to access data regarding the subject in question.

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?

Article 44 specifies that third countries must follow the regulations specified in this article even if they are not apart of GDPR.

Article 46 says that the controller or processor must enforce safeguards for such a transfer. And these safeguards must not require specific authorization from a supervisory authority.

In general all articles from 44-46 mentions data transfer.

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?

Article 28 section 3 here outlines that a contract should be written between the controller and the processor that clearly defines the subject matter and the duration. And in this contract or other legal act have several rules that the processor must follow, for example takes all measures to pursue article 32 etc.

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?

Following GDPR which has several regulations to ensure data is protected in various ways. However, specific mention of data loss is not apparent in GDPR but there are articles you can use. For example, in question 2 as few people as possible should have access to data and with fewer people having access to data the easier it is to enforce special protocols to prevent data leakage. As was also mentioned in the first question you can log user activity after accessing data so a possible insider might be aware of the risk of leaking data.

View previous incident where data leaks have occurred and use the information gained to ensure data leakage at GlobEl is prevented to such a high degree as possible.

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?

For example prevention could be using an access card on the computer to allow a user to access company information. This is done in the Swedish hospital service to allow doctors, nurses etc to take their laptops home with them. And in case a laptop is stolen the card is still needed to access sensitive patient data and therefore makes it much harder to access this data.

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?

As the company still needs to keep certain data about its users GDPR still applies to this company.

In addition Article 5, NIS 2 Directive specifies in section 2 a) that “ a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;”

Since the company is worldwide and we presume they provide services for multiple countries both within and outside of the EU several different laws might need to be followed and in the extent of this assignment all these laws will not be mentioned. Laws are applied firstly from the outside and then more inwards. So for example, first EU laws will apply and if in Sweden then specific Swedish laws might also need to be applied.

This would be the Swedish law PSA. These applies to both private and public organization therefore it applies here and that are important to sweden’s national security and infrastructure. Since it is an electrical company it is vital to infrastructure.

Some demands include that breaches need to be reported to the correct organizations (GDPR). Conduct a productive security analysis. Implement security measures based on this analysis (PSA).

And finally NIS demands that it is required to take appropriate and proportional technical and organizational measures to manage the risks posed the the security of the network.

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 was 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?

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.

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.

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 8 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

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