NAME: IWUJI CHIKAODI EDITH

REG NO: 2025/GRC/11032

GRC104: The "GlobalSync Inc." Compliance Crisis

Task 1.1: The Whistleblower Email

Allegation	Regulation/Framework at Risk	Potential Legal Implication	Key Dimension
A. Customer data from EU clients is being transferred to and processed in GlobalSync's main US data center without a proper legal mechanism	This directly goes against the GDPR, especially the rules on international data transfer under Chapter V.	The company could face a huge fine (up to 4% of annual global revenue or €20 million), serious damage to reputation, and investigation by regulators like CNIL.	This issue seems unintentional but systemic, caused by poor data governance and lack of compliance oversight across borders
B. The sales team in Brazil has been offering significant "incentives" to secure large government contracts.	This violates the FCPA (Foreign Corrupt Practices Act) and also Brazil's Clean Company Act, which both deal with bribery and corruption.	It could lead to criminal charges, heavy fines, and even imprisonment for individuals involved, plus the company might lose contracts	This one looks intentional and isolated, done deliberately by a few people within the sales department.
C. There is no centralized process for handling customer requests to delete their data, and many requests are ignored or lost.	This breaks the GDPR (Article 17 – Right to Erasure) and the CCPA/CPRA which both give users the right to request data deletion	The company could face administrative penalties, possible lawsuits, and loss of customer trust	This problem seems unintentional but systemic, because it shows a lack of proper process and oversight for handling data subject requests.
D. The company cannot reliably prove that its financial reporting controls are	This goes against the Sarbanes–Oxley Act (SOX), especially Section 404 that	It can result in financial penalties, a need to restate financial reports, and	This one appears unintentional but systemic, likely caused by weak

effective.	deals with internal control over financial reporting	loss of investor confidence.	internal control systems and poor documentation.

Task 1.2 – Risk Assessment Matrix

Likelihood \ Impact	Insignificant	Minor	Moderate	Major	Catastrophic
Rare					
Unlikely					
Possible					A,C
Likely				D	
Almost Certain				B	

Justifications for Each Allegation

A. (EU Data Transfer without Legal Mechanism)

- **Placement: Possible and Catastrophic**

- **Justification**: This issue is likely happening since GlobalSync transfers data across borders, but not necessarily known by all departments. The potential impact is catastrophic because GDPR violations can lead to fines up to 4% of annual global turnover, regulatory investigations, and loss of trust during the merger process.

B. (Bribery in Brazil – “Incentives” for Government Contracts)

- **Placement: Almost Certain and Major**

- **Justification**: The whistleblower’s description suggests the behavior is ongoing and deliberate, making likelihood very high. The impact is major

due to potential criminal prosecution under the FCPA and Brazil's anti-corruption laws, reputational damage, and costly legal settlements.

C. (Failure to Process Data Deletion Requests)

- **Placement: Possible and Catastrophic**

- **Justification**: Confirmed by audit (40% unprocessed), so this is an existing systemic issue. The impact is catastrophic because it directly violates GDPR and CCPA/CPRA "right to deletion," leading to lawsuits, fines, and severe brand damage.

D. (Weak Financial Reporting Controls)

- **Placement: Likely and Major**

- **Justification**: The inability to prove financial controls indicates probable SOX non-compliance. The impact is major because inaccurate financial statements can trigger audit failures, SEC sanctions, and loss of investor confidence, though it may not be catastrophic to the entire company.

Task 2.1 – Scoping the Audit

Scope of the Audit

The compliance audit will focus on the main business areas directly connected to the four allegations. These include:

1. **Data Protection and IT Department (EU–US Data Transfers):**
   Review how personal data from EU clients is collected, stored, and transferred to the U.S. data center.

2. **Sales and Operations Team in Brazil (Bribery Allegation):**
   Examine sales records, payment vouchers, and communication with government clients

to identify any improper incentives or bribery risk.

3. **Customer Support and Privacy Management Team (Data Deletion Requests):** Assess the current process for handling data subject requests (DSRs), focusing on whether there is a central tracking system and compliance with GDPR/CCPA timelines.

4. **Finance and Internal Controls Department (Financial Reporting Controls):** Evaluate the effectiveness of internal financial controls and evidence that supports compliance with the Sarbanes-Oxley Act (SOX).

Objectives of the Audit

- To confirm whether personal data transfers between the EU and U.S. follow legal GDPR mechanisms (such as Standard Contractual Clauses).

- To verify that sales practices in Brazil comply with the Foreign Corrupt Practices Act (FCPA) and Brazil's Anti-Corruption Law.

- To assess the adequacy and timeliness of data subject request handling in line with GDPR Article 17 and CCPA deletion rights.

- To evaluate whether GlobalSync's financial reporting controls meet SOX Section 404 standards for accuracy and accountability.

- To identify the root causes of non-compliance and recommend immediate corrective actions.

Key Audit Questions

1. What legal mechanism is currently used for EU–U.S. data transfers, and is it documented?

2. Are there any unapproved payments, gifts, or incentives recorded by the Brazilian sales team?

3. How many data deletion requests are pending, and why are they not being processed?

4. Does the finance department maintain sufficient evidence to support financial reporting accuracy?

5. What internal controls or policies are missing or ineffective across these risk areas?

Task 2.2 – Evidence Gathering Plan (Allegation A: Improper EU–US Data Transfers)

Document Review:

- Request the Data Transfer Agreement between the company and U.S. service providers.
- Review the Privacy Policy to confirm compliance with GDPR Article 44–50.
- Examine Records of Processing Activities (RoPA) to identify data flows involving EU citizens.

Interviews

Role	Key Questions
Data Protection Officer (DPO)	1. What legal basis or transfer mechanism is currently in place for EU–US data sharing? 2. How does the company monitor compliance with GDPR cross-border transfer requirements?
IT Systems Manager	1. Which systems or servers store EU customer data, and how is access controlled? 2. Are there any backup or replication processes that send data outside the EU automatically?

Legal and Compliance Manager	1. Has the company reviewed or updated its transfer agreements since the *Schrems II* ruling? 2. Are the SCCs signed and properly communicated to all EU clients?

Testing

To verify the effectiveness of GlobalSync's data transfer mechanism, the following control test is performed:

Control Test: Review a sample of actual data transfers between EU and U.S. systems using audit logs or data flow diagrams. Confirm whether each transfer has a valid legal mechanism (such as Standard Contractual Clauses or Binding Corporate Rules) attached to it.

Expected Result: Each cross-border transfer must have proper documentation and encryption, and should comply with GDPR Article 44–49 requirements. Any missing mechanism will be recorded as a control failure.

Audit Finding: Inadequate Handling of Data Subject Requests (DSRs)

Condition:
GlobalSync currently has no formal process for managing Data Subject Requests (DSRs). A review of recent activity showed that 40% of customer deletion requests were never actioned, and there is no consistent record-keeping to track DSR status or completion.

Criteria:
According to GDPR Articles 12–17, organizations must provide transparent procedures for individuals to exercise their data rights, including the right to access, rectify, and erase personal data ("right to be forgotten"). Requests must be handled promptly, typically within one month.

Cause:
The company lacks an established data privacy workflow and has not assigned specific roles or automated systems for tracking and fulfilling DSRs. Staff awareness of GDPR requirements also appears limited.

Effect:
Failure to respond to DSRs may lead to regulatory penalties, legal actions from data subjects, and damage to customer trust. It also exposes GlobalSync to potential noncompliance findings during external audits.

Risk Rating:
High. The issue directly violates GDPR requirements and affects customer personal data rights. While no public complaint has yet been filed, the high volume of unprocessed requests poses serious legal and reputational risk.

Task 3.1: The Regulator Knocks

1. Possible Mechanisms for Legal Data Transfer under GDPR (Post-Schrems II)

After the Schrems II ruling, the EU Court of Justice invalidated the EU–US Privacy Shield, meaning organizations can no longer rely on it for data transfers. However, GDPR still allows other approved transfer mechanisms, including:

- **Standard Contractual Clauses (SCCs):** Legally binding agreements between data exporters (in the EU) and data importers (outside the EU) that ensure equivalent protection for personal data.

- **Binding Corporate Rules (BCRs):** Internal policies approved by an EU regulator that allow multinational companies to transfer data within the same corporate group under consistent protection standards.

- **Derogations (Article 49):** Used for occasional or specific transfers (e.g., with explicit consent or for contract performance).

Most Robust Mechanism:
The Standard Contractual Clauses (SCCs) are currently the most practical and robust mechanism for GlobalSync to adopt. They are widely recognized by EU regulators and provide clear legal documentation for cross-border data transfers.

What GlobalSync Must Do to Implement SCCs:

- Map all existing EU–US data flows.

- Sign and document the updated 2021 EU Commission SCCs with all U.S. partners.
- Conduct Transfer Impact Assessments (TIAs) to evaluate U.S. surveillance and data protection risks.
- Apply additional safeguards such as end-to-end encryption and strict access controls.
- Maintain ongoing monitoring and periodic compliance reviews.

2. Maximum Potential Fine under GDPR

If CNIL finds GlobalSync in violation of GDPR data transfer rules, the penalty can be severe.
Under Article 83(5) of the GDPR, the maximum potential fine is:

Up to €20 million or 4% of the company's total global annual turnover, whichever is higher.

Task 3.2: The Lawsuit

1. Applicable Law and Violated Consumer Right

This lawsuit falls under the **California Consumer Privacy Act (CCPA)** as amended by the **California Privacy Rights Act (CPRA)**.
The specific consumer right that has been violated is the **"Right to Deletion."**

Under the CCPA/CPRA, California consumers have the right to request that a business delete the personal information it has collected about them (unless a specific exception applies).
In GlobalSync's case, ignoring 40% of deletion requests means the company failed to honor this legal right, which directly violates Section 1798.105 of the CCPA.

2. Difference Between the Private Right of Action (CCPA/CPRA vs GDPR)

A key difference between the two laws is how individuals can take legal action:

- Under the **CCPA/CPRA**, consumers have a limited private right of action.
  It applies mainly to cases involving data breaches caused by a business's failure to implement reasonable security measures. Other privacy violations (like ignored deletion requests) are usually enforced by the California Privacy Protection Agency (CPPA) or the Attorney General, not by individuals directly.

- Under the **GDPR**, individuals have a broader right to legal action.
  Data subjects can file complaints directly with supervisory authorities (like CNIL or ICO) or take legal action in court for any violation of their privacy rights, not just data breaches.

Task 3.3: The Settlement Dilemma

1. What is a DPA?

A **Deferred Prosecution Agreement (DPA)** is a legal arrangement between a company and government authorities (like the U.S. Department of Justice) where prosecution for a criminal offense is **suspended** as long as the company meets certain agreed-upon conditions within a set time period.
In other words, it allows the company to avoid a criminal conviction if it cooperates and takes corrective actions.

2. Two Key Benefits for GlobalSync

- **Avoidance of Criminal Conviction:**
  By accepting a DPA, GlobalSync can avoid being formally prosecuted or convicted, which protects its business reputation and ability to operate internationally.

- **Opportunity for Remediation:**
  The DPA gives GlobalSync time to correct internal compliance failures, strengthen anti-bribery controls, and demonstrate cooperation with authorities instead of facing an immediate penalty or ban.

3. Likely Obligation Under the DPA

GlobalSync will likely be required to implement a robust compliance and monitoring program.
This could include hiring an independent compliance monitor, conducting regular audits, training employees on anti-corruption policies, and submitting progress reports to the DOJ to prove sustained ethical practices.

Task 4.1: Corrective Action Plan (CAP) for Allegation C

Specific Action Items	Assigned Department/Owner	Target Completion Date	Metric for Success
1. Develop and implement a formal Data Subject Request (DSR) management policy in line with GDPR Article 12–23 requirements.	Data Protection Officer (DPO) & Legal Department	Within 60 days	DSR policy approved and communicated to all relevant staff.
2. Deploy an automated tracking system or portal to log and monitor all customer deletion and access requests to prevent loss or delay.	IT & Compliance Department	Within 90 days	100% of DSRs are logged with real-time tracking and status updates.
3. Conduct staff training and awareness programs on privacy rights and DSR handling procedures.	Human Resources & Compliance	Within 45 days	95% of staff complete training; post-training quiz score ≥ 80%
4. Perform a quarterly compliance audit to verify timely and accurate processing of data deletion requests.	Internal Audit Team	Ongoing (every 3 months)	100% of DSRs handled within 30 days as required by GDPR.

Summary:

This Corrective Action Plan ensures GlobalSync establishes a clear, automated, and accountable process for handling customer data requests. It improves legal compliance, operational efficiency, and customer trust, reducing the risk of regulatory penalties and lawsuits.

Opening Statement to the Board:

Members of the Board, compliance is not simply an expense or a legal requirement, it is a core driver of trust, growth, and sustainability for GlobalSync. As we prepare for our upcoming merger, our commitment to strong data protection, ethical business practices, and transparent governance will determine how our partners and customers view us. Investing in compliance today means securing our future, protecting our reputation, and ensuring that GlobalSync continues to grow as a company that values integrity as much as innovation.

Bonus Challenge: The Future-Proofing Question

Recommended Trend: Privacy-Enhancing Technologies (PETs)

GlobalSync should invest in **Privacy-Enhancing Technologies** such as data anonymization, encryption, and secure multi-party computation to strengthen data protection without limiting business operations. PETs help organizations process and analyze data while minimizing exposure of personal information, which is especially important for a global company managing cross-border data. By adopting PETs, GlobalSync can reduce regulatory risks, build customer trust, and stay ahead of evolving privacy requirements under laws like GDPR and CPRA. This investment will position the company as a privacy-conscious leader and prevent future crises similar to the current compliance issues.