Student Name: Oluwatimilehin Oluwagbemi

Reg. No: 2025/GRC/10712

GRC 104 The “GlobalSync Inc.” Compliance Crisis

Instructor: Miss Sharon

Date: 9th November, 2025

Part 1: The Initial Discovery & Risk Triage

Task 1.1 The Whistleblower Email

The primary Regulation/Framework at Risk:

- Allegation A: General Data Protection Regulation (GDPR)
- Allegation B: Foreign Corrupt Practices Act (FCPA)
- Allegation C: General Data Protection Regulation (GDPR) for the European Union Operations, Lei Geral de Proteção de Dados (LGPD) for the Brazil Operations and California Consumer Privacy Act (CCPA) for its California Operations.
- Allegation D: Sarbanes-Oxley Act (SOX)

The Potential Legal Implication:

- Allegation A: Financial Penalty
- Allegation B: Criminal Liability and Civil Lawsuit.
- Allegation C: Administrative Action, Lawsuits, Financial Penalty
- Allegation D: Criminal Liability, Civil Lawsuit, Financial Penalty.

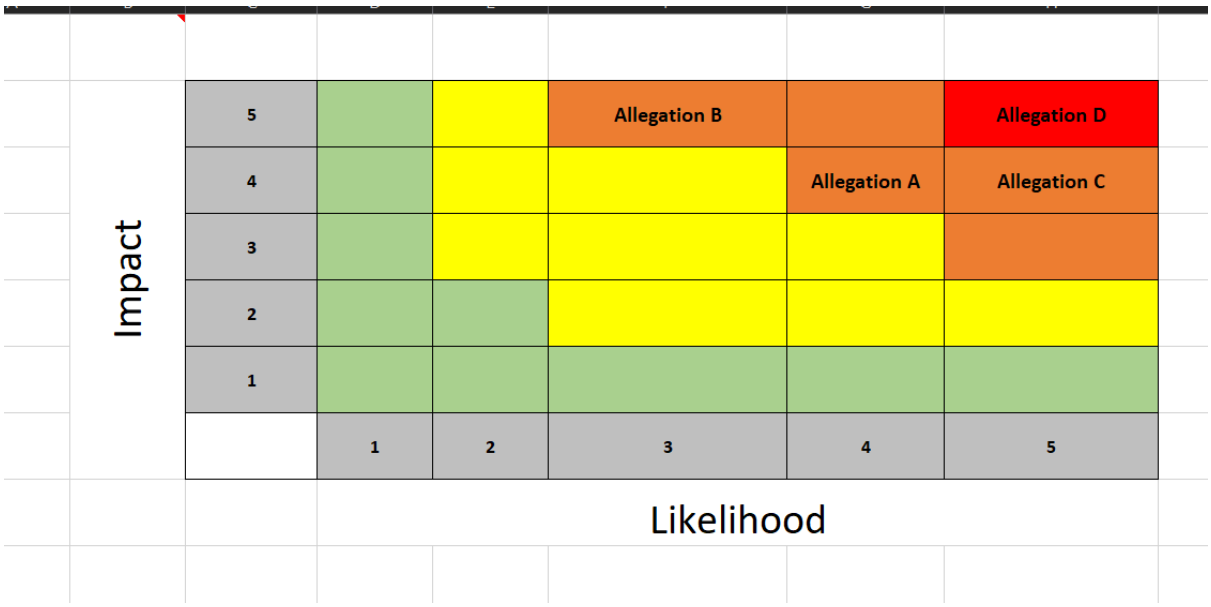
The "Key Dimension" of this Non-Compliance:

- Allegation A: it is Intentional, Systemic
- Allegation B: it is Intentional, Systemic
- Allegation C: it is Unintentional, Isolated
- Allegation D: it is Unintentional, Isolated

Task 1.2 Risk Assessment Matrix

Allegations	Likelihood	Impact	Justification
A	Likely	Major	The transfer and processing of customer data without proper legal mechanism is likely to be detected and will incur a major fine of up to 4% global turnover
B	Possible	Catastrophic	The likelihood of offering incentives to secure contracts is possible which will cause a catastrophic impact on the organization if detected
C	Almost Certain	Major	This is almost certain which might recur and incur penalties like regulatory fine
D	Almost Certain	Catastrophic	This is almost certain and can be catastrophic if fraud is uncovered, this might cause reputational damage to the organization, and regulatory fines.

The Screenshots below are the risk assessment matrix with key (Likelihood & Impact) for the potential risk GlobalSync might face (I used Microsoft Excel).



Key

Impact	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Catastrophic

Likelihood	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost Certain

Risk Impact vs Likelihood

5 and Below	Green
6 - 12	Yellow
13 - 20	Orange
25	Red

Allegations	Likelihood (L)	Impact (I)	Risk Magnitude (L x I)
Allegation A	4	4	16
Allegation B	3	5	15
Allegation C	5	4	20
Allegation D	5	5	25

Part 2: The Compliance Audit Deep Dive

Task 2.1 Scoping the Audit

The objective is to rapidly assess the veracity and scope of the four allegations, also determine the potential financial, regulatory and reputational risk to GlobalSync, especially in the light of the impending European Merger.

Business Units to examine:

- Data center operations
- Cloud Architecture
- Security
- Legal office
- Sales team
- Finance department
- Internal Audit
- IT Department

Processes and Data flows to examine:

- Data Transfer especially to European Union
- Repositories of EU customer data
- Third-Party Onboarding & vetting of contracts especially from Brazilian government

Key Audit Questions to answer:

- What is the legal basis for processing EU data in the US?
- Are there systemic failures that violates the “Right to Erasure”?
- Is GlobalSync compliant with Chapter V of GDPR (transferring of data)?
- Is the DSAR process robust, documented, and consistently followed?

- Is there sufficient due diligence on third parties involved in sales?
- Did any payments violate the FCPA, Brazilian anti-corruption laws?

Task 2.2 Evidence Gathering Plan for Allegation A (Improper EU-US data transfers)

This is where we determine if there is an existence and application of a valid GDPR Chapter V transfer mechanism. The documents requested to be reviewed are:

- Inter-company Data Transfer Agreement (IDTA) or Data Processing Agreement (DPA): this document serves as the legal contract that stipulates the valid transfer mechanisms between EU and US
- Data Inventory with focus on EU customer data: this document should state which data is being transferred, where data is being stored and which system process it.
- Transfer Impact Assessment (TIA) or Privacy Impact Assessment (PIA): according to Post-Schrems II, every EU-US transfer requires a TIA to assess local US government surveillance risks. Absence of this document poses a compliance failure.

The job roles to be interviewed with key questions for each:

- Data Protection Officer (DPO):

Q1: What is the specific legal transfer mechanism currently relied upon for the EU-US transfer?

Q2: When was the last time the associated Transfer Impact Assessment (TIA) for the US data center was reviewed and approved?

- Data Center Manager:

Q1: Can you describe the architectural and security measures (such as access controls and encryption techniques) used for EU customer data after it is stored in the US data center?

Q2: Can you provide the most recent audit report that confirms only authorized personnel (and no US government agencies) can access the data?

- Senior Compliance / Internal Audit Officer:

Q1: Has Internal Audit ever tested the compliance of the EU-US data transfer process, if so, what were the findings?

Q2: Have any employee raised internal concerns or been trained on the requirements for lawful international data transfers?

The control test to verify the data transfer mechanism:

Transfer Safeguards Effectiveness Test: this will be tested using samples of EU customer data that was recently transferred to the US data center by tracing the data path, examining the technical environment such as servers, logs, and database where the data is stored in the US. The transfer will be verified to ensure that data are encrypted using mandated cryptographic standards by IDTA, the Access Control List (ACL) must be limited to the individuals and roles documented in the IDTA, and that unauthorized IT personnel in US is systematically blocked.

Task 2.3 Drafting the Audit Finding

Formal Audit Finding: Lack of Formal Process for Data Subject Requests (DSRs)

The problem:

GlobalSync does not have a formal, centralized or documented process for receiving, tracking, verifying, or actioning Data Subject Requests (DSRs), specifically the Right to Erasure (deletion requests). A sample reveal that 40% of deletion requests were never actioned or processed.

The Criteria:

The processing and handling of DSRs, particularly the Right to Erasure, are required by the European Union's General Data Protection Regulation (GDPR). "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay," according to GDPR Article 17 (Right to Erasure). Furthermore, controllers must respond to requests "without undue delay and in any event within one month" of receipt and permit data subjects to exercise their rights in accordance with GDPR Article 12 (Transparent communication).

Root Cause Analysis:

The root cause is lack of Governance and Process Design in keeping pace with the international expansion of the company, the root cause is not limited to:

- Lack of centralized ownership: no department was assigned responsibility and accountability for the DSR process.
- Lack of Standard Operating Procedures (SOPs): no documented procedures for DSR process

Effect / Impact:

- Financial Consequences: this risk violates the core GDPR data subject right (Article 17), which equals to regulatory fine of up to €20 million or 4% of global annual turnover.
- Legal Consequences: this action makes the organization exposed to lawsuits from data subjects, especially EU customers.
- Reputational Consequences: this allegation can cause severe reputational damage to the organization, as their customers will find it difficult to trust them anymore.

Risk Rating: this risk is critical because it represents a systemic, proven, and material breach of a fundamental, high-penalty regulation (GDPR). The failure is not isolated but affects 40% of requests. Given the time-sensitive nature of the European merger, this confirmed, ongoing legal liability presents an immediate and existential threat to GlobalSync's strategic objectives and financial stability. Remediation must begin immediately before the Board can achieve any other goals.

Part 3: Navigating the Legal & Regulatory Maze

Task 3.1 The Regulator Knocks

Possible mechanisms for legal data transfer under the GDPR post Schrems II:

- EU-Us Data Privacy Framework (DPF)
- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)

The most robust mechanism can be decided based on timeline and scope, out of the above possible mechanisms, for an immediate response, the EU-US Data Privacy Framework (DPF) will be most robust because it is the fastest, simplest and most scalable route as deemed fit by the European Commission. For a long-term security, the Binding Corporate Rules (BCR) will be most robust as it offers the highest level of internal governance control and regulatory trust.

Implementation:

- Communicate the decision to rely on DPF for immediate response
- GlobalSync must self-certify their compliance with DPF principles
- Update privacy policy

Maximum Potential Fine from CNIL under GDPR is 4% of GlobalSync annual turnover or £20 million.

Task 3.2 The Lawsuit

This lawsuit falls under the California Consumer Privacy Act (CCPA) as amended in 2023 by the California Privacy Rights Act (CPRA). The specific consumer right violated is the “Right to Delete also known as Right to Erasure - CCPA / CPRA Section 1798.105”

The key difference between the private right of action in the CCPA/CPRA vs. the GDPR is that CCPS/CPRA focuses more on consumer protection and the right to control personal information as a consumer right while GDPR is based on the principle that privacy is a fundamental right.

Task 3.3 The Settlement Dilemma

A Deferred Prosecution Agreement (DPA) is a voluntary contractual agreement between the United State Department of Justice (DOJ) and a corporation facing criminal Charges.

The two key benefits for GlobalSync in accepting DPA:

- DPA will make it possible for GlobalSync to avoid criminal conviction and collateral damage
- DPA will mitigate financial penalties if accepted.

One major obligation GlobalSync will likely fulfil under DPA is appointing a Compliance Officer.

Part 4: The Strategic Roadmap & Board Presentation

Task 4.1 The remediation plan

Corrective Action Plan (CAP)

S/N	Specific Action Item	Assigned Department/Owner	Target Completion Date	Metric for Success
1	Establish Centralized Governance & Accountability	Chief Compliance Officer (CCO)	2 Weeks	The Executive Committee's formal approval of the DSR Response Team Charter, which explicitly defines roles, responsibilities, and decision-making authority for DSR management (i.e., transferring DSR ownership from Support to Legal/Privacy).
2	Full Backlog Remediation & Customer Communication	IT Operations / Chief Privacy Counsel	4 Weeks	100% of the genuine, misplaced, or inactive DSRs from the 12-month backlog have been identified and fulfilled.
3	Implement Dedicated DSR Management System & SOPs	VP of IT/Cloud Operations / Chief Privacy Counsel	8 Weeks	All requests must be submitted through the live, integrated dedicated DSR Management Software Platform (SaaS). 100% of the DSR Response Team has finished the required training, and Standard Operating Procedures (SOPs) for DSR fulfillment have been issued.
4	Post-Implementation Audit & Effectiveness Testing	Internal Audit	12 Weeks	The effectiveness of the new DSR process and system (both in terms of design and functionality) is confirmed by the Internal Audit Report. Within the allotted 30-day period, the first 30 days of live operation must demonstrate a consistent 99% fulfilment rate with no lost or missed requests.

Task 4.2 The “Tone at the Top”

Opening Statement

One thing has become evident as a result of the whistleblower's tip and the CNIL and DOJ's subsequent regulatory actions: compliance is now our biggest strategic asset and a vital enabler of high-growth business, not just a check-the-box expense. According to my analysis, there are serious systemic issues that could jeopardize this company. However, by implementing these corrective actions immediately, we will move from reactive crisis management to proactive governance, protecting our valuable brand, our legal position, and most importantly, ensuring the successful completion of the merger, which will position GlobalSync for long-term, ethical growth.

Bonus Challenge:

I will recommend Continuous Auditing, because it cuts across all the allegations discovered by the whistleblower. Investing in Continuous Auditing will enable GlobalSync monitor necessary compliance regulatory to adhere to as the auditing will cut across all departments, they will be able to monitor which data is being transferred and how.