Ex 5.3 Data Ethics: Data Security and Privacy
Lisa Coombs
February 19, 2025

Step 1 Money Laundering at Pig E Bank

Is this a data privacy issue, a data security issue, or both?	**What would be the risks to Pig E. Bank and its customers if this issue weren't addressed?**	**To prevent this type of data theft in the future, what changes would need to be made to the policies around data access?**
This is mostly a data security issue. The investigator should not be taking photos of the computer screen that displays sensitive PII and customer account information. This could lead to data leaks or fraud. This is a data privacy issue as well because it violates privacy regulations, not only at the bank, but in other regulations like the GDPR.	The bank could face regulatory violations resulting in fines and legal consequences, thereby compromising their trust and business practices with the public. Fraud because the stolen customer information could be used for identity theft. This is also a ank security breach because if employees take sensitive information outside the company, it could be hard to track.	Train all employees on the data handling policy, prohibit the use of personal digital equipment like phones when interacting with the data. Require written acknowledgement of security measures before they can access account information and PII.

Step 2 Outsourcing some lower-level analytical functions to a contractor in a foreign country

Does this scenario highlight a data privacy issue, data security issue, or some other ethical issue?	**How would you communicate your concerns to the compliance committee?**	**If Pig E. Bank does go ahead and outsource some of its analytical functions, how would you anonymize the data while ensuring that someone can still conduct an analysis?**
It primarily raises data privacy concerns with some ethical implications. Outsourcing sensitive low-level analytical functions to a contractor in a foreign country may expose personally identifiable information (PII) including details such as pay grade, address, and contact information—to countries with potentially lower data protection standards. This risk is further compounded by the inclusion of active military personnel in the bank's customer base, where its exposure could lead to national security concerns. Cost-saving benefits are attractive, but the potential compromise of customer privacy and trust represents a significant ethical issue that must be considered carefully.	I would communicate my concerns to the compliance committee: Risk assessment outlines the risks associated with outsourcing sensitive data that could be a potential violation of data privacy regulations (like GDPR). Emphasize the sensitivity of the data in question. These records include highly sensitive PII, including the PII of military personnel, which may require additional regulatory or national security concerns. Reference Industry Best Practices by presenting examples where similar outsourcing led to data breaches.	Using "differential privacy" to anonymize the data that would be outsourced. It injects "noise" into the quantitative data associated with a customer to the point where the customer can no longer be identified in the data output. Other ways are encryption, firewalls, passwords and clear policies that define who can access the data and how it is to be handled.

Ex 5.3 Data Ethics: Data Security and Privacy
Lisa Coombs
February 19, 2025

Step 3 How do other countries deal with data ethics?

Research a case study from your country where a company or organization has unethically collected and shared data. (Include link to resources)	**Explain what the company or organization did. Did they act according to regional or national laws?**	**Why was the company's behavior unethical? (To answer this question, refer to this Exercise and the previous Exercise on data bias.)**	**What could the company have done to prevent this unethical behavior?**
Cambridge Analytica: The story so far From 2014 to 2015, Cambridge Analytica obtained personal data from millions of Facebook users through a personality quiz app. Users did consent to share their data; however, they were not informed that their information would be passed onto a third party for political profiling. The data harvested through the personality quiz app was later used during the 2016 US Presidential election to influence voter behavior.	Cambridge Analytica exploited regions, like in the US, that had less strict or even not so clear regulations on data privacy. However, in the UK, where GDPR is active, these practices were in violation of the standard for data protection and ethical data handling.	Cambridge Analytica was, in fact, unethical with the handling of the data harvested from the personality quiz app. It violated Informed Consent by not fully disclosing that the data harvested would be used for political purposes. This undermined transparency in data handling and collection. This incident breached the trust of digital platforms across the board. It highlights how the misuse of personal data can have negative consequences on privacy and the US democratic election processes.	Enhance transparency by clearly communicating to users how their data will be collected, shared and used. Obtain explicit informed consent before sharing data with third parties. Implement data governance that outlines strict internal policies that align with internation standards like GDPR. Audit data collection on a regular basis and share practices to ensure compliance with legal and ethical standards. Develop internal accountability measures that address deviations from ethical standards.

BONUS

Have you ever faced an ethical concern at work?	**If yes, what was the situation, and what was your concern?**	**How did you deal with it?**
In my role as a category manager, I handled sensitive information that spanned several key departments—including procurement, kitchen operations, culinary R&D, beverage and bakery, quality assurance, legal, and finance. My responsibilities involved managing pricing data and contract details specific to the products and vendors I sourced.	Due to the confidential nature of this information, my primary ethical concern was ensuring that sensitive pricing and contractual data remained secure and was only accessible to the intended department. Any exposure of this information could have led to competitive disadvantages, internal conflicts, or even regulatory issues.	**Paperless Workflow:** I transitioned to digital documentation wherever possible. This not only reduced the risk of physical data leaks but also streamlined the secure storage and retrieval of sensitive information through controlled access systems. **Monitor Protector:** I installed a monitor protector to minimize the risk of visual hacking. This ensured that confidential information on my screen could not be easily viewed, especially in open or shared office spaces. **Strict Information Sharing Protocols:** I maintained clear boundaries regarding data access. Sensitive pricing and contract information was shared strictly on a need-to-know basis, reinforcing a culture of confidentiality and ensuring that only relevant departments had access.