Step 1: Read the following scenario and answer the questions

Your role at Pig E. Bank is to develop models that detect suspicious account activity associated with money laundering. Your current project requires you to distribute prototype model outputs to your team of investigators for validation. Standard investigation procedure requires the investigator to access client PII and account information to build a customer profile before dispositioning the model output. One day, you notice one of your investigators taking a photo of his screen while sensitive client data is displayed.

- Is this a data privacy issue, a data security issue, or both? Please provide a short explanation for your answer.

This is a data security issue, that then affects the privacy of the data.

We don't know what will happen to that data on the phone – it is now outside of the bank's security procedures. And that might mean privacy could be compromised.

- What would be the risks to Pig E. Bank and its customers if this issue weren't addressed?

The investigator now has personal possession of PII that they should not.

The bank may be shown to not be protecting its data sufficiently – and may be in breach of the law

The customer's details are now less secure, and they are more at risk of data crime

- To prevent this type of data theft in the future, what changes would need to be made to the policies around data access?

Investigators should only have access to data they absolutely need, and perhaps even then the ACTUAL data need not be made available to them, just the anonymised categories.

Policy should be in place and applied to everyone with this data access about they should or should not do.

If there is a risk that this may be prevalent, then phones or other devices could be banned when accessing this kind of data.

Step 2: Read the following scenario and answer the questions

Your manager has asked you to join them in representing the compliance analytics department at the compliance committee meeting. At the meeting, the prospect of outsourcing some lower-level analytical functions to a contractor in a foreign country is discussed, and it is popular with the other department heads. Outsourcing could save the bank millions of dollars annually in labor costs, and the department heads seem confident that this won't violate data privacy laws. You know from experience that some of your bank's customers can be identified as being on active military duty, and, like all clients, you keep records of their pay grade, address, contact information, and other PII.

- Does this scenario highlight a data privacy issue, data security issue, or some other ethical issue? Explain your answer.

There is an ethical concern about the decision to move jobs away from your home country – but that is outside of the remit of this!

Investigations need to be done on their own privacy and security standards, with assurances they can meet or exceed those that would be followed in the home country. There would need to be an ongoing checking that they are maintaining those standards. It may be worth getting regulatory advice on how this is managed.

Security may be better ensured by only sharing information they absolutely need – and perhaps by anonymising other information

- How would you communicate your concerns to the compliance committee? To answer this question, you can rely on either your previous work experience or the tips provided in the Exercise, but be as specific as you can.

I would talk about the responsibilities and process that we have in place in the Bank. I would talk about how, regardless of the fact that we are outsourcing some analysis, we remain entirely responsibly for the security of that data. I would look to weigh up the potential savings of the move vs the cost of even one data breach.

Of course, it might be my own job that is at risk, so I need to be detached and independent. Expert, external opinions or sources may prove valuable.

- 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? (Use the information and resources provided in the Exercise to answer this question; there's no need to go into technical details.)

There may be no need to provide the PII alongside the information – that would be the simplest and most secure way to keep data safe and protect the bank and customers

OR we may not need to provide ALL of the data. If for instance they just need to know pay grade and military service, this will not make any individuals identifiable, and there is much less risk from sharing this data.

It could be that we just assign customers and ID number. This could mean that a lot of the low level analysis is outsourced, and only one re-insourced is the PII applied in an environment we know is more secure.

Step 3: Read the following scenario and answer the questions

Suppose you've lived and worked in different cities around the world, and you're interested in learning more about how other countries have dealt with data ethics.

- Research a case study from your country where a company or organization has unethically collected and shared data. You're free to use information you find online, but make sure you include the link to your resources in your document.
- Explain what the company or organization did. Did they act according to regional or national laws?

https://www.digital-adoption.com/data-ethics-examples/

Tech giant Google has come under fire several times over the years for its unethical data use.

In 2020, a lawsuit was filed against Google's parent company, Alphabet Inc. The lawsuit claimed users browsing the web via Google Chrome's "Incognito" and "Private" browser modes were unknowingly tracked.

Even with private browsing enabled and location tracking disabled, data collection methods continued. User data was collected via Google websites and apps, device location data, and third-party cookies and analytics.

Plaintiffs of the lawsuit claim that the company's practices "give Google and its employees power to learn intimate details about individuals' lives, interests, and internet usage; and make Google "one-stop shopping" for any government, private, or criminalactor who wants to undermine individuals' privacy, security, or freedom." The case eventually settled in 2024, with Google ordered to pay $5 billion.

Similarly, in 2019, Google was found to be collecting data on children under the age of 13 via YouTube, a subsidiary of the company.

The COPPA (Children's Online Privacy Protection Act) stipulates that data collected via websites, apps, and online services directed at children or knowingly collecting information must obtain parental consent beforehand. The Federal Trade Commission (FTC) fined Google $170 million in response to these breaches.

Examples like these reiterate how even industry-leading firms aren't immune to unethical data use. To avoid financial penalties and remain compliant, today's companies must establish transparency and adhere to non-negotiable rules regarding user data collection.

- Why was the company's behavior unethical? (To answer this question, refer to this Exercise and the previous Exercise on data bias.)

With the incognito/private browser example, there is a clear lack of transparency. Usres are using these tools precisely because they do not want this data to be collected and yet Google was doing just that.

In the YouTube example, law specifically prohibits collection of data from children – who are presumably not able to give consent in the same way as adults. Without this consent, there is no true privacy for the person involved.

- What could the company have done to prevent this unethical behavior? Please provide some concrete suggestions.

Google needed to either NOT collect data when users were in incognito/private browser OR make it far clearer what that function actually meant in terms of data collection, and obtain specific consent for that data to be collected.

In the YouTube example, there needed to be far more stringent processes on the collection of data – possibly to the extent that if they did not know the age of users, they should not collect data at all. (I presume they did not do that – if they needed to do that, I assume there would be a far greater level of sign-in needed on You Tube, otherwise they would not have data from (presumably) a large majority of their users who are casually viewing.