# 4.4 Ethical and Social Issue

***Types of data collected by the travel agency***

As a travel agency, the Personal data that is collected includes all kinds of sensitive data, ranging from: Personally identifiable information (PII) as full names, passport numbers, travel details, contacts, and credit card data. Possibly, some medical or accessibility requirements may be collected. This information is critical to making flight reservations, accommodation bookings and personalized services for the customers. However, there arises a great concern with respect to data privacy and security when dealing with such data. Left exposed to cyber threats such as unauthorized access to data, data breaches, identity theft, and financial fraud, it becomes susceptible to harm if not protected well enough.

***Privacy and security concern***

The primary concerns revolve around:

* Unauthorized Access: Once this data is accessed by the internal or external parties without authorization.
* Data Breaches: Incidents of leaks, thefts, and exposures of customers’ information as a result of poor security practices.[[1]](#footnote-1)
* Misuse of Data: Use of data inappropriately for example, use of data for marketing purposes without consent or sale of the same to third parties.

The possibility of the existence of vulnerabilities may exist without strong security controls in:

* Unsecured data transmission channels
* Poor access control of internal systems
* Outdated software on on-premise servers

***Legal and Regulatory Implication***

The agency has to adhere to:

* Australia’s Privacy Act 1988: Governs personal information collection, storage and use with an aim to ensure privacy to individuals in Australia.[[2]](#footnote-2)
* Australian Privacy Principles (APPs): Provide guidelines to agencies as to how personal information should be dealt with in a transparent manner with security measures in place and accountability.
* General Data Protection Regulation (GDPR): EU regulation, which provides for data privacy of people in the EU for international clients of the agency.
* Notifiable Data Breaches (NDB) scheme: Requires notification of the individuals who are affected and the Office of the Australian Information Commissioner if there happens to be a significant data breach.[[3]](#footnote-3)

***Impact of Data Breach***

The consequence of a data breach can be tremendous on all the involved parties. For the customers, the consequences will include risks for them to become victims of identity theft and fraud and even experience emotional distress, which is likely to erode the level of confidence that the agency could properly protect the private data of the customers. The agency is at risk of being tarnished in its reputation and losing its customers’ confidence, as well as potential regulatory fines or lawsuits. These impacts can bring long-term financial and operational ramifications.[[4]](#footnote-4) In addition, if the personal or HR data of the staff members is compromised, they may be affected, which may raise concerns about privacy and possible legal action. Therefore, ethical practice in handling data and the establishment of strong security systems a crucial aspects in keeping trust, compliance, and protection against such risks.

1. <https://www.researchgate.net/publication/335002124_The_Effect_of_Data_Breaches_on_Company_Performance> [↑](#footnote-ref-1)
2. <https://www.msocialsciences.com/index.php/mjssh/article/view/1766> [↑](#footnote-ref-2)
3. <https://www.researchgate.net/publication/374611237_Australia's_Notifiable_Data_Breach_Scheme_An_Analysis_of_Risk_Management_Findings_for_Healthcare> [↑](#footnote-ref-3)
4. <https://journals.sagepub.com/doi/10.1177/21582440231181395?icid=int.sj-abstract.citing-articles.157> [↑](#footnote-ref-4)