**Reflective Activity**

As a Data Scientist at Attitude Group of Hotels in Mauritius, my role comprises of analysing complex datasets to enhance guest experiences across our nine diverse properties. Leveraging advanced analytical techniques, I provide insights that shape strategic decisions, from optimizing pricing models to personalizing guest services. My work significantly influences targeted marketing and operational efficiency, aligning with Attitude Group's commitment to sustainable, technology-driven hospitality. The company, known for its eco-friendly and authentic Mauritian hospitality, relies on data-driven strategies to maintain its competitive edge and uphold its reputation as a leader in the innovative hospitality sector.

One of the largest industries that caters primarily to people is the hospitality industry. Hotels, restaurants, and resorts have enormous databases that contain information about business operations as well as information about customers that visit the restaurant or resort. The collection of data in the hospitality sector begins at the reservation stage, where personal information ranging from generic data like names and phone numbers to sensitive data like bank account details is gathered. Moreover, nowadays, The Internet of Things (IoT) offers various opportunities to improve hospitality operations, most notably by enhancing operational efficiency and customer satisfaction through massive data collection (Car et al., 2019). These businesses gather substantial volumes of personal data. While the industry has significantly benefited from online booking systems, mobile apps, and data analytics, this digital transformation entails the generation, collection, and processing of substantial data.

In the hospitality industry, guest privacy is a critical concern, particularly regarding the collection, use, and protection of guest data. Data is essential for creating guest profiles to enhance experiences, improve operational efficiency, and for marketing purposes, as noted by Mercan et al. (2020). However, the protection of this data is paramount. Unauthorized access and breaches pose risks of identity theft, financial loss, and can significantly harm the hotel's reputation. Therefore, implementing stringent security measures to protect guest data is not only a legal necessity but also crucial for maintaining customer trust and the integrity of the hotel's brand. Mishandling guest data in the hospitality industry can have severe repercussions, including legal penalties, erosion of guest trust, and detrimental effects on brand reputation. Implementing robust data protection measures, as highlighted in the HRS Column (2023), is both a legal mandate and an ethical obligation.

A common issue is having disjointed visitor profiles across multiple systems like PMS, CRM, and POS, leading to manual updates and security risks. Implementing a Central Data Management (CDM) system or a fully integrated software solution, to create unified, secure customer profiles and ensure real-time synchronization of data, enhancing protection against data breaches (Merlin, 2022). Also, ensuring guest privacy in the hospitality sector involves robust measures like data encryption and strict access controls. Conducting regular audits of data protection practices and educating staff on privacy's importance are critical (HRS Column, 2023). Additionally, managing how guest data is shared with third parties is equally vital. Ethical handling requires careful consideration when dealing with entities like travel agents and booking platforms to prevent unauthorized data access or misuse. This comprehensive approach to privacy strengthens trust and compliance with privacy standards.

Consent and transparency in data collection are crucial in the hospitality industry under GDPR's Articles 6 and 7. Guests must be clearly informed about what data is collected, why it's needed, and how it will be used, ensuring an understanding of their data's purpose. Crucially, guests should have the option to consent to or opt out of marketing communications, request data transfers, and exercise the “right to be forgotten.”, a practice that aligns with ethical standards and legal mandates. This approach not only adheres to legal requirements but also fosters trust and respect between hotels and their guests, reinforcing the importance of guest autonomy in data-related decisions.

Another primary concern is data security. According to a Trustwave cybersecurity report published in 2023, Nearly 31% of hospitality organisations have reported a data breach in their company’s history with the average cost of a breach at around US$3.4m. These events underscored the critical need for enhanced data security in the hospitality sector, leading to increased regulatory attention and the implementation of comprehensive security programs (PwC, 2016). The rise of technology in hotel operations, such as IT systems and IoT for guest services, has further accentuated the importance of robust cybersecurity measures. As hotels become more reliant on digital technologies to enhance guest experiences, the risk of data breaches also escalates, making the protection of guest information a paramount concern. This focus on data security is not just about safeguarding information; it's also about maintaining guest trust, which is directly linked to the industry's revenue and reputation. Consequently, the hotel industry has been compelled to strike a balance between leveraging technological advancements and ensuring the safety and confidentiality of guest data, a balance that is crucial for the industry's long-term success and customer loyalty (Shabani, 2020).

To ensure data security in the hospitality industry, several best practices are employed. These include encrypting payment card data, often coupled with two-factor authentication to prevent unauthorized access and identity theft. Employee training on data storage and handling is critical to mitigate insider attacks. Cybersecurity measures such as firewalls, traffic filters, and network monitoring are implemented to protect against online malware. Regular testing of computer systems by businesses is conducted to assess the effectiveness of cybersecurity providers. Additionally, tracking data across various systems is crucial for monitoring and safeguarding the movement of sensitive information (Devi, 2023).

In the hotel industry, data security and guest privacy transcend mere compliance and risk management, intertwining with the economic benefits of using personal data for customer insights and personalized services. Developing a clear Vision that aligns economic goals with risk management and legal compliance is crucial. This Vision should reflect the unique attributes of the entity and consider all stakeholders' perspectives. A strategic plan based on this Vision can guide the establishment of necessary structures. Failures in data handling often stem from a lack of such a Vision. Hotel security and privacy professionals should evaluate if their organization has this Vision and collaborate with stakeholders to advance their strategies.

References:

T. Car, L. P. Stifanich, and M. Simuni ˇ c, “Internet of things (iot) in ´ tourism and hospitality: Opportunities and challenges,” Tourism in South East Europe..., vol. 5, pp. 163–175, 2019.

J.-E. Pelet, E. Lick, and B. Taieb, “Internet of things and artificial intelligence in the hotel industry: Which opportunities and threats for sensory marketing?” in International Conference on Advances in National Bran

Art. 5 GDPR – principles relating to processing of personal data (2021) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/art-5-gdpr/ (Accessed: 25 December 2023).

Mercan, S. et al. (2020) ‘Security, privacy and ethical concerns of IOT implementations in hospitality domain’, 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) [Preprint]. doi:10.1109/ithings-greencom-cpscom-smartdata-cybermatics50389.2020.00048.

Moon, H. et al. (2022) ‘Hotel Privacy Management and guest trust building: A relational signaling perspective’, International Journal of Hospitality Management, 102, p. 103171. doi:10.1016/j.ijhm.2022.103171.

Collins, E. (2023) Why data privacy matters in the hospitality sector, EasyMerlin. Available at: https://easymerlin.com/why-data-privacy-matters-in-the-hospitality-sector/ (Accessed: 30 December 2023).

Wainstein, L. (2023) Data Security in hospitality: Risks and best practices, Hospitality News & Business Insights by EHL. Available at: https://hospitalityinsights.ehl.edu/data-security-in-hospitality-best-practices (Accessed: 30 December 2023).

Shabani, N. and Munir, A. (2020) ‘A review of cyber security issues in hospitality industry’, Advances in Intelligent Systems and Computing, pp. 482–493. doi:10.1007/978-3-030-52243-8\_35.

Devi, N. (2023) Data Security in the hospitality industry: Post-COVID ERA, loginradius. Available at: https://www.loginradius.com/blog/identity/data-security-hospitality-industry/#data-security-concerns-for-the-hospitality-business (Accessed: 30 December 2023).

Law, M. (2023) Trustwave report on Hospitality Industry Security threats, Cyber Magazine. Available at: https://cybermagazine.com/articles/trustwave-report-on-hospitality-industry-security-threats (Accessed: 30 December 2023).

(2016) Cyber and data security in the hotel industry - PWC. Available at: https://www.pwc.com/m1/en/publications/documents/cyber-and-data-security-in-the-hotel-industry.pdf (Accessed: 30 December 2023).