TASK 3

Sophie Fidan 21068639

UFCFU3-15-3
Advanced Databases

TABLE OF CONTENTS

DATA SECURITY & PERSONAL DATA

Data security is the practice of protecting data against unauthorised usage or theft throughout its life cycle. Ensuring confidentiality, integrity, and availability is crucial for any system.

This becomes especially critical when handling personal data, which refers to any information that can identify a living individual, known as the 'data subject' (GDPR, 2018). This data can hold a wide range of details, some of which may not directly identify an individual but can do so when combined with other information. For example, a street name paired with a city may be sufficient to pinpoint an individual, even without mentioning their name. Given the sensitive nature of personal data, strong data protection is particularly essential for individuals' privacy, preventing abuse, and guaranteeing compliance with legal requirements such as the General Data Protection Regulation (GDPR).

IMPACT ON DATABASE DESIGN AND PERFORMANCE

The use case database stores sensitive personal information such as names, emails, dates of birth, addresses, and preferences. It is therefore necessary to abide by data privacy laws and protect the data stored in the database.

The Database Management System

The Database Management System (DBMS) is a software solution to manage databases while ensuring data integrity and security. DMBS can achieve data protection through the following mechanisms:

Encryption

Encrypting data at rest and in transit using cryptographic algorithms is required to prevent unauthorised access.

Encryption at Rest: Encrypting data in the database ensures that even if the storage media is compromised, the data remains protected. This is achieved by using database-level encryption or by encrypting individual fields (ICO, 2023b).

Encryption in Transit: Encrypting data in transit ensures that data is protected while transmitting between clients and servers over the network. Protocols like Transport Layer Security (TLS) for database connections make this possible (ICO, 2023b).

Access Control

Access control provides user authentication to regulate who can view or use resources in a computing environment so that only authorised persons can access sensitive data. It is implemented with access control lists (ACL) and role-based access controls (RBAC) by creating users with specific privileges and roles (Rahim, 2022).

Flow Control

Flow control regulates the distribution or flow of information among accessible objects, maintaining data confidentiality. This can be accomplished by preventing unauthorised transfers between security levels (Chefranov,2022).

Inference Control

Inference control prevents users from deducing sensitive information from the data. For example, in the use case, if users need to analyse the information, there is a risk that they could infer individual data points. To mitigate this, the system can restrict the statistical queries, queries that involve statistical aggregate functions, thereby protecting personal data (Chefranov,2022).

Database Auditing

Database auditing logs all database activities to monitor access patterns, detect unauthorised access, identify potential security breaches and provide an audit trail for regulatory compliance.

Pseudonymisation

Pseudonymisation means replacing identifiable information with pseudonyms (EDPB, 2025). This allows data to be re-identified as necessary but makes it more difficult for unauthorised users to identify individuals. Although pseudonymisation is not directly a DBMS feature, the DBMS can facilitate its implementation through hashing or masking techniques. One example for the use case can be replacing email addresses with unique identifiers or pseudonyms:

person1@email.com → person1@private.com

While these techniques reduce the impact of data breaches, they require additional processing and storage, which can affect database performance (Gomes et al., 2021).

Database Administrator

Database Administrator (DBA) is the responsible person who interacts with DBMS to enforce and monitor security policies. The DBA manages the user privileges by creating and assigning roles, conducts regular audits to ensure compliance with regulations and detects any unauthorised access or anomalies. Additionally, DBA performs regular backups and recovery to protect data against loss.

LEGAL ISSUES

Business failure to comply with data regulations faces significant financial penalties. Therefore, the database must obtain detailed logs of data access and modifications, as well as allow individuals to request access, rectify or delete their data (ICO, 2023a).

BUSINESS REQUIREMENTS

Ensuring data security aligns with business requirements to protect customer trust and maintain a positive reputation. Secure handling of personal data can also be a competitive advantage, as customers are more likely to engage with businesses that prioritize their privacy and security.

RISK ASSESSMENT

Risk assessment is the process of analysing the potential risks associated with the organisation's database. The effectiveness of security measures is maintained through regular reviews of the risk assessment and ongoing database monitoring.

For the use case, the following steps can be taken:

1) Identifying sensitive information (e.g., names, emails).
2) Determining potential threats (e.g., unauthorised access, data breaches and malware).
3) Assessing vulnerabilities (e.g., outdated software, weak passwords)
4) Evaluating the likelihood and impact of each threat.
5) Categorising the risks as low, medium or high.
6) Implementing mitigation measures.

REFERENCES

1. Chefranov, A. (2022) *Database Security Control Measures* [course materials for CMSE512]. Spring 2022. Available from: https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE512/Spring%202022/Database%20Security%20Control%20Measures.docx [Accessed 25 March 2025].

2. EDPB (2025) *Guidelines 01/2025 on Pseudonymisation*. 16 January 2025 [online]. Available from: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf [Accessed 24 March 2025].

3. GDPR (2018) *Personal Data General Data Protection Regulation* [online]. Available from: https://gdpr-info.eu/issues/personal-data/ [Accessed 24 March 2025].

4. Gomes, A., Santos, C., Wanzeller, C. and Martins, P. (2021) Database Encryption for Balance Between Performance and Security. *Journal of Information Assurance & Cybersecurity* [online]. pp. 1–9. Available from: https://ibimapublishing.com/articles/JIACS/2021/614511/ [Accessed 24 March 2025].

5. ICO (2023a) *A Guide to Individual Rights*. 24 May 2023 [online]. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/ [Accessed 24 March 2025].

6. ICO (2023b) *Encryption*. 19 May 2023 [online]. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/encryption/ [Accessed 24 March 2025].

7. Rahim, J. (2022) MongoDB vs MySQL: Which One Should You Choose? *Astera* [blog]. 5 September 2022. Available from: https://www.astera.com/type/blog/mongodb-vs-mysql/ [Accessed 24 March 2025].