

Unit 8 to 10: Compliance, DBMS AND APIs

Overview

In these units, I explored key areas that connect data protection, system design, and secure API development. Some of the core learning points included:

- What data stakeholders are expected to comply with regarding legal and ethical data use.
- The rights individuals have over how their data is collected, stored, and used.
- The standards and frameworks that guide data protection and privacy—such as the GDPR and NDPA.
- Activities that fall under regulation and the industries most impacted.
- Core concepts that underpin database design and management.
- The role of database management systems (DBMS), their strengths, weaknesses, and best-fit environments.
- How APIs are used to fetch, share, and integrate data across systems.
- Security risks associated with APIs and the measures required to keep them stable, secure and reliable.

Comparing Compliance Laws: GDPR and Global Equivalents

One of the major tasks was to critically evaluate how the GDPR's security principle compares with similar laws in other countries. Article 32 of the GDPR, supported by guidance from the UK's Information Commissioner's Office (ICO), makes it clear that personal data should be protected using appropriate technical and organisational measures—such as encryption, access control, and system resilience (ICO, n.d.).

In my analysis, I compared this to **Nigeria's Data Protection Act (NDPA, 2023)**. The NDPA is a significant improvement on previous regulations, bringing Nigeria closer to international standards. It mirrors the GDPR in areas like breach notification timelines, oversight, and enforcement, and is regulated by the newly established Nigeria Data Protection Commission (NDPC).



Initial Post

by Chiamaka Ndudirim - Friday, 18 July 2025, 3:53 PM

The GDPR's security principle requires that personal data be processed in a way that ensures appropriate protection, covering risks like unauthorised access, loss, or damage. It calls for technical and organisational safeguards, such as encryption, access controls, and regular risk assessments (ICO, n.d.). In the UK, this is enforced by the ICO, which also outlines certain exemptions for journalism, national security, and public interest.

Nigeria's Data Protection Act, 2023 (NDPA) builds on the earlier NDPR (2019) and introduces a much stronger framework. It establishes the Nigeria Data Protection Commission (NDPC) and clearly defines what is expected in terms of data security. Similar to the GDPR, it includes requirements for breach notification within 72 hours, proactive risk assessments, and system resilience measures (NDPA, 2023). However, the NDPA gives the NDPC more flexibility to grant exemptions based on context, while still applying broadly to both public and private sectors.

Overall, both frameworks share a focus on accountability, confidentiality, and integrity, but the NDPA marks a big step forward for Nigeria by aligning more closely with global standards and giving regulators more structure to enforce data security across industries.

References

ICO (n.d.) *Security*. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/security/> (Accessed: 17 July 2025).

NDPA (2023) *Nigeria Data Protection Act*. Available at: <https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf> (Accessed: 17 July 2025).

From my peers' insights:

- **Thailand's PDPA** shares several GDPR principles but allows broad government exemptions under Section 4, weakening accountability (DLA Piper, 2025).
- **Saudi Arabia's PDPL** is still developing and lacks specific breach timelines, which can lead to uncertainty in enforcement (Alshammari and Simpson, 2023).
- **UK GDPR**, while still closely aligned with the EU version, is gradually diverging post-Brexit. The ICO continues to lead enforcement, but international data transfer rules are evolving (Wired, 2020).

A key point that stood out was how differently **exemptions** are handled. GDPR's exemptions are narrow and usually tied to specific safeguards. In contrast, other frameworks like the PDPA and PDPL grant broader carve-outs for public authorities, creating inconsistency in protection.

References

Alshammari, M. and Simpson, A. (2023) 'PDPL vs. GDPR: A Comparative Analysis of Data Protection Laws in Saudi Arabia', *Journal of Information Policy*, 13(1), pp. 85–104.

DLA Piper (2025) *Data protection laws of the world: Thailand*. Available at: <https://www.dlapiperdataprotection.com/?c=TH> (Accessed: 17 July 2025).

ICO (n.d.) *Security*. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/security/> (Accessed: 17 July 2025).

NDPA (2023) *Nigeria Data Protection Act*. Available at: <https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf> (Accessed: 17 July 2025).

Wired (2020) *What is GDPR? The summary guide to GDPR compliance in the UK*. Available at: <https://www.wired.com/story/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018/> (Accessed: 19 June 2025).

API Security Requirements Task

We were also asked to evaluate the security requirements of an API and write a short specification to address risks related to sharing, scraping, and connecting a Python program to formats like XML, JSON, or SQL.

My submission focused specifically on **JSON**, where I outlined best practices such as:

- Using secure authentication and role-based access control.
- Validating JSON input with strict schemas.
- Avoiding risky functions like `eval()` and using safe parsing methods like `json.loads()`.
- Keeping responses minimal and applying rate limiting and general error handling.

You can view the full task here:

<https://github.com/TechieMaks/eportfolio.github.io/blob/d5ff6c9bafa1bed9380c45b3d4435c87fc7e0055/API%20Security%20for%20JSON.pdf>

Core Readings

Schiller, R. and Larochelle, D. (2024) *Data Engineering Best Practices*. Sebastopol, California: O'Reilly.

Tejada, Z. (2024) *Big data architectures*.

Wired. (2020) *What is GDPR? The summary guide to GDPR compliance in the UK*

Recommended Readings

McKinney, W. (2022) *Python for Data Analysis: Data Wrangling with Pandas, NumPy, and Jupyter*. 3rd edn. Sebastopol, California: O'Reilly.

- Chapters 11, 12, 13 and 14.