# Unit 8 to 10: Compliance, DBMS AND APIs

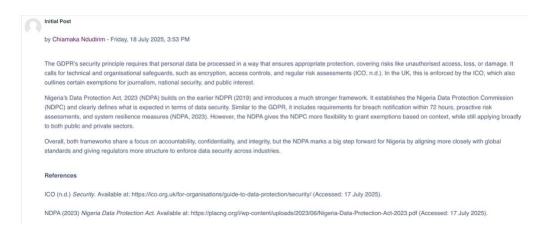
#### **Overview**

These units tied together data protection, database design, and secure API development. Key takeaways included:

- What data controllers and processors are responsible for under data protection laws
- Rights individuals have over how their data is collected and used
- Frameworks like GDPR and NDPA that shape compliance
- How **DBMS** work, their pros and cons, and when to use them
- How APIs allow systems to exchange data—and the risks that come with it

# **Comparing Compliance Laws: GDPR vs Others**

A major task was evaluating how **GDPR's security principles** compare with global counterparts. Article 32 of the GDPR (ICO, n.d.) calls for strong technical and organisational safeguards. I compared this to Nigeria's **NDPA (2023)**, which aligns with GDPR on breach reporting, enforcement, and individual rights, and is now regulated by the **NDPC**.



#### From my peers' insights:

- **Thailand's PDPA** is similar to GDPR but offers broad government exemptions (DLA Piper, 2025).
- Saudi Arabia's PDPL is still evolving and lacks set breach reporting timelines (Alshammari and Simpson, 2023).
- UK GDPR is diverging post-Brexit but still largely aligns with the EU framework (Wired, 2020).

The biggest difference lies in **how exemptions are handled**. GDPR's are narrow and tied to strict conditions. Others, like PDPA and PDPL, give more leeway to public authorities, which can weaken data protection.

#### **API Security Requirements Task**

We were asked to write a brief **API security requirements spec**, focused on preventing issues when sharing data between a Python app and formats like JSON, XML, or SQL.

When working with APIs that handle JSON, security needs to be a priority—especially when dealing with user data. JSON is fast and flexible, but without the right safeguards, it can open the door to data leaks or attacks.

### **Key Points:**

- **Secure Access**: Only authenticated users should access or send data. Role-based access helps restrict visibility to just what users need (OWASP, 2017).
- **Input Validation**: Always validate JSON payloads with tools like pydantic or jsonschema to prevent malicious or malformed data (Shetty, 2019).
- **Safe Parsing**: Use json.loads() instead of risky options like eval(), and avoid sending sensitive data like passwords or tokens in responses (Kissel, 2013).
- Rate Limiting: Control how often endpoints can be hit and avoid exposing system details in error messages (OWASP, 2017).

## Final Thoughts:

JSON is great for sharing data, but security isn't automatic. By validating inputs, limiting exposure, and applying the right controls, APIs become more reliable and safer for users.

#### 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: <a href="https://www.dlapiperdataprotection.com/?c=TH">https://www.dlapiperdataprotection.com/?c=TH</a> (Accessed: 17 July 2025).

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

Kissel, R. (2013) *NIST Special Publication 800-53 Revision 4:* Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology.

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

OWASP (2017) OWASP REST Security Cheat Sheet. Available at: <a href="https://cheatsheetseries.owasp.org/cheatsheets/REST\_Security\_Cheat\_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/REST\_Security\_Cheat\_Sheet.html</a> (Accessed: 21 July 2025).

Shetty, R. (2019) 'Securing APIs with JSON Schema', *InfoQ*. Available at: <a href="https://www.infoq.com/articles/securing-apis-json-schema/">https://www.infoq.com/articles/securing-apis-json-schema/</a> (Accessed: 21 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).