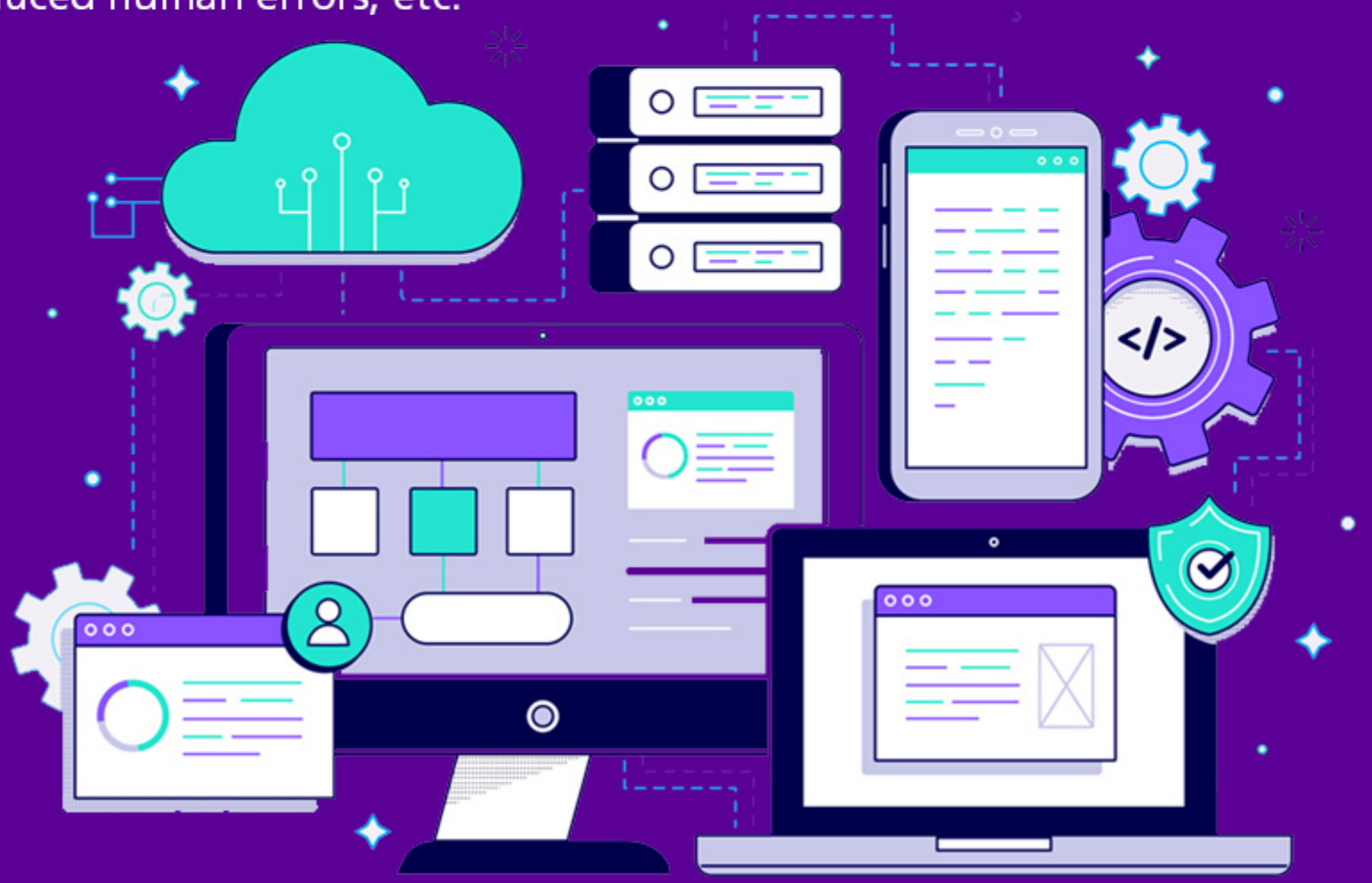
DUALE, OVIA & ALEX-ADEDIPE

API: Legal Protection for Technology Connections

Understanding APIs

Application Programming Interface ("API") are sets of protocols and standards that permit different software applications (or platforms) to communicate with each other. API integration refers to the process of connecting two or more applications or systems to exchange data and perform certain actions. Practically, two applications can be connected to each through their API to perform some joint function for the benefit of the business owner or the end-users. When a user logs onto websites or other platforms using Google or Facebook accounts, the action is made possible through API integration.

Businesses rely on API integrations to streamline processes, connect systems and sync data so as to improve efficiency and service delivery. The benefits of API integration include automation, enhanced end-user experience, improved functionality, reduced human errors, etc.



Technology Sectors and API Integrations

Sector	Function/Examples
Financial Services	Online banking, payment gateways, and financial data aggregation.
E-Commerce	Payment processing, online orders placement, integration of mapping APIs to track the delivery in real-time, inventory management, and third-party integrations with logistics providers.
Telecommunications	Customer relationship management tools and systems.
Insurance Industry	Real-time policy issuance, claims processing. API integration facilitates communication between insurers and insurtech platforms.
Logistics and Transportation	Route optimization, real-time tracking of shipments, and seamless collaboration between logistics partners in the supply chain.
Human Resources and Recruitment	Digital resume screening and applicant tracking.

Legal Protections for API Integrations

1. API License Agreements:

Technology companies should ensure that they enter into agreements that clearly define the terms and conditions governing API license and usage. These agreements specify the permissible actions, usage scope, and associated fees. It is common for API agreements to include clauses prohibiting actions like reverse engineering to protect the underlying/source code. Additionally, incorporating provisions for liabilities and indemnity helps safeguard the API provider from potential legal issues or misuse by the business or third parties.

2. Intellectual Property Rights:

API providers often retain intellectual property ("IP") rights over their APIs. Agreements must clearly define the IP rights related to the API and specify ownership of the API, any associated software, and any modifications or improvements made during integration. An IP assignment clause may be inserted to cater for any developments to the API by a third party. This ensures that the provider retains ownership of any improvements made in the course of the integration. API documentation, code, and associated trademarks are also protected under IP laws. For example, the Copyright Act 2022 defines computer programmes as literary works which are eligible for copyright protection.

3. Data Security and Privacy:

API providers must prioritize data security and privacy when dealing with API integrations. It is essential to comply with data protection laws, such as Nigeria Data Protection Act 2023 and the subsidiary legislations. API providers may impose restrictions on the type of data that can be accessed, processed, or shared with a third party. They must ensure that necessary consent is obtained for processing personal data, and for cross border transfers where applicable.

4. Terms of Use and Acceptable Use Policies:

API providers should establish terms of use and acceptable use policies that end-users must adhere to. These policies are guidelines to end-users regarding the dos and don'ts related to the API usage. Violating these terms can result in the rightful termination of access to the API.

5. Service Level Agreements (SLAs):

The SEC Regulatory Incubation Guideline (the "**Guideline**") provides a framework that allows FinTech companies (whose activities may or may not be subject to existing regulations) to carry out capital market activities for a limited period of time without prior registration with SEC. Similarly, the CBN's Regulatory Framework for Sandbox Operations (the "**Framework**"), provides for the operation of a sandbox dedicated to the Nigerian payment services system and is focused on promoting innovation in the design and delivery of products, services, or solutions that are either not contemplated under the extant laws and regulations or do not precisely align with the extant laws and regulations.

6. Non-Disclosure Agreements (NDAs):

NDAs safeguard API integration by establishing confidentiality commitments between the connecting parties. They define the scope of protected information, ensuring clarity on what constitutes sensitive data. Confidential information may include data exchanged during the integration as well as the APIs, source codes, etc. In the event of a breach, NDAs provide a legal foundation for seeking remedies and deter unauthorized disclosure, fostering trust in the exchange of technical information during integration.

Conclusion

As digital ecosystems expand, businesses increasingly rely on API integrations to drive innovation and business growth, by linking technology and forging profitable partnerships. Consequently, it is paramount to establish robust legal protections in API integrations. Legal protections help to safeguard end-user data, comply with regulations, and establish clear contractual frameworks.