Global Data Privacy and Governance Policy

Document ID: LC-DPP-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: Legal & Compliance, IT Security

1. Scope and Applicable Laws

This policy applies to all NexaCore personnel and covers all personal data (PD) collected, processed, and stored globally. We adhere to the stricter of the applicable standards, including but not limited to:

- **EU General Data Protection Regulation (GDPR)**
- **UAE Federal Decree Law No. 45/2021 (PDPL)**
- Specific regulatory requirements in KSA and Egypt (e.g., data localization, foreign data transfer).

2. Key Data Principles

Principle	Definition
Lawfulness, Fairness, and Transparency	Data processing must have a clear legal basis, be transparent to the data subject, and be done fairly.
Purpose Limitation	Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
Data Minimization	Only PD that is adequate, relevant, and limited to what is necessary for the purposes of processing shall be processed.
Accuracy	PD must be accurate and, where necessary, kept up to date.
Storage Limitation	PD must be kept for no longer than is necessary for the purposes for which the PD is processed (see **Data Retention**

	Schedule).
Integrity and Confidentiality	PD must be processed securely, protected against unauthorized access, and accidental loss or destruction.

3. Regional Data Localization Requirements (MENA)

- **UAE (PDPL):** PD can generally be transferred outside the UAE provided the destination country ensures an adequate level of protection, or adequate safeguards are in place (e.g., specific contractual clauses).
- **KSA and Egypt:** Specific client contracts and regulatory instructions may mandate certain sensitive data (e.g., government data, financial data) be hosted **only** within the national borders. The Product team must use regional server clusters to comply with these requirements.

4. Data Subject Rights

NexaCore must have mechanisms to respond to Data Subject Access Requests (DSARs), including the right to access, rectify, erase ("right to be forgotten"), and restrict processing of their PD. All DSARs must be routed to the Compliance Officer within **[48 hours]** of receipt.