DPA Guard – Sample SME Playbook

This Playbook defines acceptable, fallback, and red-flag positions for reviewing Data Processing Agreements under GDPR (Articles 28–32).

DPA-SEC-01 – Security Measures

Requirement: Specific technical and organizational measures must be described or referenced.
Red Flag: Vague statements like 'appropriate measures' with no detail.
Fallback: Reference to ISO 27001 or equivalent security framework.

DPA-SUB-01 – Subprocessors

Requirement: Advance notice and right to object to new subprocessors.
Red Flag: Unrestricted use of subprocessors with no notice.
Fallback: General authorization with prior notification.

DPA-TR-01 – International Transfers

Requirement: Clear transfer mechanism (SCCs, adequacy decision).
Red Flag: Transfers allowed with no safeguards mentioned.
Fallback: SCCs incorporated by reference.

DPA-BR-01 – Breach Notification

Requirement: Notification within a defined timeframe (e.g., 72 hours).
Red Flag: 'Without undue delay' with no timeframe.
Fallback: Notify within 72 hours of awareness.

DPA-DEL-01 – Deletion/Return

Requirement: Explicit obligation to delete or return data after termination.
Red Flag: No deletion clause or retention at processor’s discretion.
Fallback: Deletion within a defined period (e.g., 30 days).