JANUS COMPLIANCE

Sample DPIA Structure for an AI Chatbot

Redacted sample deliverable for buyer review. Not client-specific advice.

This is a redacted outline showing the structure Janus Compliance uses when documenting an AI chatbot or similar AI system under GDPR.

1. System Summary

• What the system does

• Who uses it

• Business purpose

• Core vendors and infrastructure

2. Roles, Lawful Basis, and Scope

• Controller / processor map

• Lawful basis by processing purpose

• Article 9 or child-data issues

3. Personal Data Inventory

• Direct user inputs

• Logs and metadata

• Outputs and derived data

• Retention periods

4. Data Flow and Transfer Map

• Entry points

• Storage locations

• Model providers

• Cross-border transfers

• DPAs and SCCs

5. Risk Assessment

• Unauthorized access

• Excessive collection

• Over-retention

• Unsafe outputs

• Transfer risk

6. Controls and Mitigations

• Minimisation

• Human oversight

• Logging

• Access controls

• Retention rules

7. Residual Risk and Sign-Off

• Residual risk level

• Review frequency

• Approval and ownership

This outline is not legal advice and should not be used as a drop-in template.