

CHECKLIST ACCOUNTABILITY & GOVERNANCE



This checklist helps organisations demonstrate accountability and governance in line with the DPJL 2018 and DPAJL 2018. Use it to evidence compliance, identify gaps, and record ongoing improvements.

1. GOVERNANCE & LEADERSHIP

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Senior management formally endorses data protection strategy and policy.		
Clear, up-to-date internal privacy policy in place (with regular review).		
Privacy notice(s) available and accurate.		

2. ROLES & RESPONSIBILITIES

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Data Protection Officer (DPO) or equivalent appointed with appropriate independence and resources.		
Roles and responsibilities for data protection are clearly defined and documented.		

3. DATA INVENTORY/MAPPING

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Record of Processing Activities (RoPA) maintained and reviewed regularly.		
Data flow diagrams include all internal and external transfers.		



4. RISK & IMPACT ASSESSMENT

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
DPIAs conducted for new or high-risk processing activities.		
Data protection risks identified and documented in a risk register.		

5. POLICIES & PROCEDURES

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Policies exist for retention, deletion, access, breach, and data subject rights.		
Processor contracts are in place and include all required data protection clauses.		

6. TECHNICAL & ORGANISATIONAL MEASURES

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Appropriate security, confidentiality, and integrity controls implemented.		
Privacy by design and by default applied to new projects.		

7. TRAINING, AWARENESS & CULTURE

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Regular staff training on data protection responsibilities.		
Privacy awareness promoted across the organisation.		



8. MONITORING, AUDITING & REPORTING

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Internal audits or reviews conducted periodically.		
Metrics (e.g. DSARs, breaches, audits) reported to senior management.		

9. DATA SUBJECT RIGHTS & TRANSPARENCY

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Mechanisms in place to respond to DSARs and other subject rights (rectification, erasure etc.) within statutory deadlines.		
Privacy notices reviewed and updated periodically.		

10. BREACH & INCIDENT MANAGEMENT

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Incident response plan tested and reviewed regularly.		
Breach log maintained; corrective actions documented.		

11. THIRD PARTY & TRANSFER GOVERNANCE

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Vendor oversight and audits conducted.		
International transfers assessed and safeguarded appropriately (e.g. SCCs plus Jersey Addendum, adequacy).		



12. CERTIFICATION & ACCOUNTABILITY TOOLS

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Organisation considers certification, codes of conduct, or seals to demonstrate compliance.		

13. CONTINUOUS IMPROVEMENT & DOCUMENTATION

REQUIREMENT/QUESTION	COMPLIANT (YES/NO/PARTIAL)	EVIDENCE/NOTES
Privacy framework reviewed annually or when laws/processing change.		
Evidence of compliance documented and readily available for the JOIC.		