DPO Caribbean

Data Retention & Disposal Compliance Checklist

1. DATA INVENTORY
☐ Identify all personal data processed
☐ Identify storage locations (paper, systems, cloud, backups, devices)
☐ Identify responsible departments or roles
☐ Identify third parties or service providers handling personal data

2. LAWFUL RETENTION
☐ Confirm the purpose for collecting each data category
☐ Retain data only as long as necessary for that purpose
☐ Identify data required for legal or regulatory record-keeping
☐ Identify data retained for legal claims
☐ Document any legitimate business reasons for extended retention

3. RETENTION & DISPOSAL POLICIES
☐ Maintain a written retention and disposal policy
☐ Define minimum and maximum retention periods
☐ Specify disposal triggers (e.g. contract end, legal expiry)
☐ Apply policies to physical and electronic records
☐ Communicate policies to staff

4. REGULAR DATA REVIEWS
☐ Conduct periodic reviews of personal data holdings
☐ Identify data no longer required
☐ Assign responsibility for reviews
☐ Include archived and backup data
☐ Dispose of unnecessary data promptly

5. DECISION-BASED DATA
☐ Identify data used to make decisions about individuals
☐ Retain such data for a reasonable post-decision period
☐ Allow time for data access requests
☐ Document retention periods

6. SECURE DISPOSAL
☐ Ensure disposed data cannot be further processed
☐ Ensure disposed data cannot identify an individual
☐ Use disposal methods appropriate to data sensitivity
☐ Ensure electronic data disposal is permanent
☐ Securely shred or destroy physical records

7. TECHNOLOGY & FUTURE RISK
☐ Assess whether deleted data could be recovered
☐ Consider foreseeable technological developments
☐ Update disposal methods as systems change

8. THIRD-PARTY MANAGEMENT
☐ Require service providers to follow compliant disposal practices
☐ Include disposal obligations in contracts
☐ Confirm disposal timelines and methods

9. DOCUMENTATION & ACCOUNTABILITY
☐ Keep records of retention decisions
☐ Document disposal actions and methods
☐ Be able to demonstrate compliance to regulators
☐ Review and update policies regularly

10. TRAINING & AWARENESS
☐ Train staff on retention and disposal obligations
☐ Reinforce that “delete” ≠ secure disposal
☐ Encourage reporting of data handling issues

KEY REMINDER:
Personal data must not be kept longer than necessary and must be disposed of securely and permanently once no longer required.