CHECKLIST SURVEILLANCE SYSTEM DEPLOYMENT

Businesses & Organisations

This checklist is provided for general guidance. It is intended to help you consider whether CCTV is necessary and, if so, whether its use complies with relevant data-protection and legal requirements. It should be adapted to your specific circumstances and is not a substitute for formal legal advice.

You remain responsible for ensuring that any CCTV system you install or operate is necessary, proportionate, and compliant with all relevant data-protection and legal requirements.

SECTION 1 - PRELIMINARY ASSESSMENT

□ Define the purpose: clearly document and explain why surveillance is needed and ensure no less intrusive means exist.

□ Identify your lawful basis under Schedule 2 of the DPJL 2018.

□ Assess necessity and proportionality of system coverage, retention, and angles.

□ Carry out a Data Protection Impact Assessment (DPIA) for high-risk deployments (e.g., drones, public areas, staff monitoring). Make sure it covers:

- Purpose & necessity
- Data types collected
- Risks to individuals
- Mitigation measures
- Retention, access, deletion
- Keep it under review and re-do it for any system changes.

□ Assign responsibility: nominate a responsible person, consult your DPO, update ROPA, and consult JOIC if unsure and/or if required.

SECTION 2 - DESIGN & PROCUREMENT

□ Design the system/choose equipment to minimise intrusion and ensure privacy embedded by design and default (masking zones, limited resolution, encryption).

□ Provide clear and prominent signage stating controller, purpose, contact info, and link to privacy notice.

□ Execute any necessary Data Processing Agreements with installers, hosting providers, or monitoring service providers.

□ Implement encryption, access control, password/MFA protection, and maintain access logs.

□ Keep devices up-to-date and physically secured.

□ Define retention periods, automatic deletion, and log retention exceptions.

SECTION 3 - DEPLOYMENT & OPERATION

□ Train staff who operate or view footage. Keep a record of training provided.

□ Publish a CCTV/surveillance policy outlining scope, access, deletion, and misuse sanctions.

□ Provide/make privacy notices available. If cameras cover staff or visitors, notify them explicitly (e.g. staff handbook, visitor notices).

□ For drones or mobile units, publish online notice and post area signage..

□ Prepare to handle subject access, erasure, objection, and restriction requests within statutory times. Keep a record of all requests and outcomes.

□ Implement breach response policy and ensure staff know what to do in the event of a breach (including notifying th JOIC within 72 hours if risk to individuals is likely).

□ Review system annually: reassess necessity, effectiveness, retention, and decommission/destroy any obsolete data/equipment. Document any review and update any DPIA/ROPA as required.

SECTION 4 - TECHNOLOGY-SPECIFIC ADD-ONS

□ Drones/UAVs: Register with CAA Jersey, plan safe flight paths, use geofencing and altitude limits, avoid private properties, enable recording control.

□ ANPR: Limit capture to number plates, avoid occupants, maintain short retention and audit logs.

□ Body-worn video: Record only during incidents, use visible indicator lights so people know when they're recording, and train staff on activation.

□ Audio recording: Capture only if strictly necessary, use explicit signage, and avoid continuous recording.

SECTION 5 - REQUIRED DOCUMENTATION

□ Surveillance Policy – Defines scope, responsibilities, retention, and data subject rights.

□ Data Protection Impact Assessment (DPIA) – Demonstrates necessity, proportionality, and safeguards.

□ Privacy Notice – Transparency for data subjects.

□ Processor Agreement – Legal contract for third-party providers.

□ Retention Schedule & Log – Duration and deletion records.

□ Access Log – Records all footage access/export events.

□ Breach/Incident Log – Evidence for JOIC and internal audit.

□ Annual Review Record – Reassesses ongoing need and compliance.