CROWD-SENSE

Data Protection Impact Assessment template

For organisations deploying Crowd-Sense passive Wi-Fi pedestrian-density sensors

Pre-populated against the Information Commissioner's Office accountability framework and Article 35 UK GDPR. Sections in **PRE-FILLED** *are pre-filled with Crowd-Sense processor information that is the same for every deployment. Sections in* **CONTROLLER TO COMPLETE** *are for the controller (your organisation) to complete with your venue-specific information. Document version 2026-04-25.*

How to use this template

This template is structured to satisfy Article 35 UK GDPR requirements for a Data Protection Impact Assessment when processing involves systematic monitoring of a publicly accessible area on a large scale. Even where a DPIA is not strictly mandatory, the ICO recommends one be undertaken for any Wi-Fi location analytics deployment.

The processing Crowd-Sense supports is, by architecture, low-risk: device identifiers are discarded on the sensor and only aggregate counts ever leave it (see `DPO_TECHNICAL_NOTE.pdf` and `TECHNICAL_SPECIFICATION.pdf`). However the brief on-device processing of a probe-request MAC may itself be personal data on the singling-out test, so a DPIA is the prudent posture.

Roles in this template:

- **Controller** — your organisation (council, BID, retailer, workplace facilities team) deploying the sensors at your venue. You determine the purpose and means of processing.
- **Processor** — Crowd-Sense, providing the sensor and the hosted analytics platform on your behalf, under Article 28 processor terms.

Complete the **CONTROLLER TO COMPLETE** sections, sign off at the end, and retain. Provide a copy to your Data Protection Officer.

Section 1 — Identification and contact information

1.1 Name of the project / processing activity **CONTROLLER TO COMPLETE** *e.g. "Town centre pedestrian density measurement, Phase 1, 2026–2031"*

1.2 Data controller **CONTROLLER TO COMPLETE**

- Organisation name:
- Registered address:
- ICO registration number (if applicable):
- Data Protection Officer name and contact:

1.3 Data processor PRE-FILLED

- Trading name: Crowd-Sense
- Legal entity: **Visual Solutions UK Limited** (Companies House #02955160)
- Status: Active; incorporated 3 August 1994
- Primary DPO contact: dpo@crowd-sense.com
- Director: Jeff Burton (jeff.burton@crowd-sense.com)
- Article 28 processor terms entered into: *date to be filled in by controller*

1.4 DPIA assessor and date CONTROLLER TO COMPLETE *Name, role, date completed*

Section 2 — Description of the processing

2.1 Nature of the processing

PRE-FILLED Passive reception of 802.11 management frames (probe requests and beacons) broadcast by Wi-Fi-enabled devices in proximity to a sensor. For each probe request, the source MAC address and received signal strength are held briefly in volatile memory of the sensor. At the close of each aggregation time window (1, 5, 15, 30 and 60 minutes, running in parallel), the unique MAC addresses observed within that window are binned into RSSI distance brackets, the per-bracket counts are emitted as a compact JSON record, and the underlying MAC hashmap for that window is deleted.

The wire payload is approximately 110–130 bytes per record, totalling approximately 10 KB per hour per sensor. It contains aggregate counts and bracket edges only, and no identifier of any kind that could attribute observations to a person or device.

No image, audio, vehicle classification, or biometric data is captured. No active interrogation or transmission to nearby devices occurs. Reception is passive.

2.2 Scope of the processing

CONTROLLER TO COMPLETE

- Number of sensors deployed: *e.g. 15*
- Geographic coverage: *e.g. central pedestrianised zones of [town]*
- Estimated number of data subjects affected per day: *e.g. 30,000 unique devices observed per day across the network*
- Duration of deployment: *e.g. 5-year contract Oct 2026 to Sep 2031*

2.3 Context of the processing

CONTROLLER TO COMPLETE

- Source of the data: passive reception in publicly-accessible space
- Relationship with data subjects: *none — passers-by are unaware of the sensor and have no relationship with the controller*
- Data subjects' likely awareness and expectations: *to be considered against signage and venue-context norms*
- Any prior concerns or incidents: *e.g. none / specific incident*

2.4 Purposes of the processing

CONTROLLER TO COMPLETE *e.g.:*

- Measurement of pedestrian density in [town centre / venue / floors] for the purpose of evidencing the [BID delivery plan / cabinet paper monitoring / workplace utilisation programme]
- Provision of operational data to inform [event scheduling / cleaning rotas / safety planning]
- Reporting to [stakeholders / cabinet / works council] under [scheme / agreement]

Section 3 — Necessity and proportionality

3.1 Lawful basis for processing

CONTROLLER TO COMPLETE *Select and justify:*

- ☐ Article 6(1)(e) UK GDPR — public task (typical for councils, BIDs, public-sector authorities)
- ☐ Article 6(1)(f) UK GDPR — legitimate interest (typical for retailers, private workplaces, commercial venues; requires legitimate interest assessment)
- ☐ Article 6(1)(c) UK GDPR — legal obligation (rare)

3.2 Special category data

PRE-FILLED No special category data (Article 9 UK GDPR) is processed by the system. The data captured is a Wi-Fi MAC address (held transiently on the sensor, discarded at window close) and signal strength. Neither attribute reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health, sex life, or sexual orientation.

3.3 Children's data

PRE-FILLED Not specifically targeted. Children may broadcast probe requests from their devices in the venue area; the data minimisation and anonymisation measures applied (on-device aggregation, MAC discard) apply equally regardless of the data subject's age.

3.4 Necessity assessment

CONTROLLER TO COMPLETE Could the controller achieve its stated purpose without this processing? Consider:

- Manual counting (limitations: cost; sustainability; coverage)
- Camera-based footfall counting (privacy concerns; CCTV-code obligations; cost)
- Mobile-SDK location-data subscription (consent-chain risk; supplier-side methodology dependency; recent regulatory enforcement)
- Telco aggregator data (granularity limitation; tile-scale resolution)

State why the chosen approach (passive Wi-Fi probe sensing with on-device aggregation) is the least-intrusive available option that achieves the purpose.

3.5 Proportionality

PRE-FILLED

- The on-device aggregation step ensures that no identifier is retained beyond the longest aggregation window (60 minutes), and that nothing identifying any individual is ever transmitted off the sensor.
- The wire payload is by design the minimum necessary to achieve the purpose: aggregate counts per distance bracket per time window.
- Processing is proportionate by data-minimisation-by-design (Article 25 UK GDPR).

3.6 Information rights

CONTROLLER TO COMPLETE How will the controller satisfy data subject rights?

- ☐ Transparency / right to information — venue signage at all entrances and prominent locations within the deployment area; web-page reference on the controller's website. Signage artwork supplied by Crowd-Sense.
- ☐ Right of access — controller may certify in writing that no personal data exists in the controller's or processor's systems for the requester to access, because all probe-request MACs are discarded on the sensor within 60 minutes of capture.
- ☐ Right to erasure — applies trivially: the data is already deleted by design within 60 minutes of capture.
- ☐ Right to object — opting out of being counted requires the data subject to disable Wi-Fi on their device (not under the controller's control); the controller may explain this on the signage.

Section 4 — Risks to the rights and freedoms of data subjects

For each potential risk, complete: likelihood, severity, overall risk score, and the mitigating measure.

#	Risk	Likelihood	Severity	Overall	Mitigation
R1	A specific individual's presence, dwell, or movement is identified	Very low	Medium	**Low**	**PRE-FILLED** On-device aggregation, MAC discard at window close, wire payload contains no identifier. Architecturally not possible.
R2	Aggregate data is misinterpreted as unique-visitor counts and published with overstated confidence	Medium	Low	**Medium**	**PRE-FILLED** Methodology statement and overcount table provided to the controller (`METHODOLOGY_AND_ACCURACY.pdf`); cite-able paragraph supplied for use in any public-facing report.
R3	Sensor is physically tampered with to attempt capture of probe data before aggregation	Very low	Low	**Low**	**PRE-FILLED** Sensor is mains-powered with continuous network telemetry; tamper would be detected within minutes. Storage and transit are encrypted.
R4	Network compromise exposes wire payload	Medium	Very low	**Low**	**PRE-FILLED** Wire payload is aggregate counts only. No personal data exposure even on full compromise. HTTPS with certificate pinning protects against transit interception.
R5	Processor security failure exposes platform-side data	Low	Very low	**Very low**	**PRE-FILLED** Platform stores only aggregate counts; processor security incident cannot expose personal data because none is held.

#	Risk	Likelihood	Severity	Overall	Mitigation
R6	Data subjects unaware their devices are being counted	High	Low	**Medium**	CONTROLLER TO COMPLETE Venue signage installed at all entrances and prominent locations; web-page reference. Controller to confirm signage installation as deployment-readiness condition.
R7	Re-identification through a future regulatory or technological change	Very low	Medium	**Low**	PRE-FILLED No identifier persists for re-identification to operate on. Mitigation is permanent by architecture, not policy.
R8	Children's devices included in counts	High	Very low	**Low**	PRE-FILLED Counts are aggregate, no per-device profile possible. Same data-minimisation as for adult data subjects.
R9	CONTROLLER TO COMPLETE *Add controller-specific risks here*				

Section 5 — Mitigation summary and residual risk

PRE-FILLED Mitigations applied by architecture (not subject to controller deviation):

- On-device aggregation; MAC discard at window close
- No off-device identifier of any kind, raw or hashed
- Encrypted transit (HTTPS with certificate pinning)
- Aggregate-only platform storage
- Subject Access Request response factually no-data-held
- Right to erasure satisfied by design

CONTROLLER TO COMPLETE Mitigations applied by the controller (you):

- ☐ Venue signage installed and maintained
- ☐ Web-page reference describing the processing
- ☐ Article 28 processor agreement signed with Crowd-Sense
- ☐ Internal staff briefing on what is and is not measured
- ☐ Annual review of this DPIA

Residual risk after mitigation: CONTROLLER TO COMPLETE *Low / Medium / High — assess and justify*

Section 6 — Outcome and sign-off

6.1 DPO advice CONTROLLER TO COMPLETE *Insert DPO's written opinion. Standard form: "I have reviewed this DPIA and consider the residual risk to data subjects' rights and freedoms to be [LEVEL]. The processing may proceed [WITH / WITHOUT] additional measures."*

6.2 Decision CONTROLLER TO COMPLETE *e.g. "The Council has decided to proceed with the deployment as described, subject to the controller-side mitigations listed in Section 5."*

6.3 Sign-off CONTROLLER TO COMPLETE

Role	Name	Date	Signature
DPIA Author			
Data Protection Officer			
Senior Information Risk Owner / equivalent			

6.4 Review schedule CONTROLLER TO COMPLETE This DPIA will be reviewed annually, and immediately following any:

- Change in the scope or scale of the deployment
- Change in the processor's architecture (notified via processor change-control)
- New regulatory guidance materially affecting the processing

---

Appendix A — Reference documents

- *Crowd-Sense — Technical privacy note for Data Protection Officers* — the compliance argument for the architecture
- *Crowd-Sense — Technical specification* — the architectural detail (under NDA)
- *Crowd-Sense — Methodology and accuracy* — the published overcount disclosure
- ICO 2016 *Wi-Fi Location Analytics* guidance
- Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques (WP216)
- UK GDPR Article 35 (Data Protection Impact Assessment requirements)
- ICO accountability framework

This template is provided to support the controller's compliance with UK GDPR Article 35. Completion of the DPIA is the controller's responsibility. Crowd-Sense assists with technical detail and processor-side information but does not act as legal counsel. Where in doubt, the controller should seek independent advice.