CROWD-SENSE

Crowd-Sense — Technical privacy note for Data Protection Officers

How a passive Wi-Fi pedestrian density sensor stays outside the definition of personal data

For DPOs reviewing a proposed Crowd-Sense deployment under UK GDPR / GDPR / equivalent. Not a contractual document. Verifiable claims correspond to the firmware behaviour described in the product technical specification, available under NDA on request.

Quick read

1. **MAC addresses never leave the sensor.** They are processed on-device for ≤60 minutes and discarded at aggregation close. They are not hashed, salted, pseudonymised or transmitted.
2. **Only aggregate bracket counts are emitted** — approximately 10 KB per hour per sensor of integer counts per RSSI distance bracket per time window. No identifier of any kind, raw or transformed, traverses the network.
3. **The wire payload is not personal data** because it cannot single out, link to, or infer about any individual. It aligns with the safe-harbour described in the Information Commissioner's Office (ICO) 2016 guidance *Wi-Fi Location Analytics* and meets the three-pronged anonymisation test of Article 29 Working Party Opinion 05/2014 (WP216).

1. What the sensor does

A Crowd-Sense sensor is a small mains-powered ESP32 device (M5Stack Atom family). It listens passively on 802.11 channels 1–13 for management frames — primarily probe requests broadcast by nearby mobile devices searching for known networks, plus occasional beacon frames. It does not interrogate any device, broadcast probes, deauthenticate clients, or interfere with traffic in any way. It receives only what is voluntarily broadcast into open RF space.

Because reception is passive, the sensor does not "store information on, or access information stored on, the terminal equipment of a user," and Article 5(3) of the ePrivacy Directive (transposed in the UK as PECR Regulation 6) is therefore not engaged. This is the established analysis for passive probe listening (Bird & Bird 2016; Pinsent Masons 2016).

2. The on-device aggregation pipeline

Inside each sensor:

1. A probe request is captured. Its source MAC address, RSSI value, and timestamp are held briefly in volatile memory.

2. Five parallel time windows run concurrently (1, 5, 15, 30 and 60 minutes), each with its own MAC hashmap.
3. At each window close, the unique MACs present in that window's hashmap are binned into five RSSI distance brackets (default edges −50/−60/−70/−80 dBm, mapping to ≤3 m / 3–8 m / 8–15 m / 15–25 m / fringe). The sensor emits one JSON object containing **only**: window length, window-close timestamp, bracket edges, and a count per bracket.
4. **The MAC hashmap for that window is then deleted.** Not hashed, not salted, not archived — discarded. The sensor retains no record that the device was seen.

The wire payload is approximately 110–130 bytes per window-close, totalling roughly 10 KB per hour per sensor. There is no per-device persistence beyond a maximum 60-minute on-device retention. There is no persistent fingerprint, recurring identifier, or device hash anywhere downstream.

This is materially different from the architecture used by every Wi-Fi-analytics vendor that has been the subject of regulatory enforcement: those products retain hashed or salted MACs in a back-end database to enable longitudinal tracking. **Crowd-Sense has no back-end MAC database. There is nothing to retain.**

3. Why the wire payload is not personal data

Article 4(1) UK GDPR defines personal data as "any information relating to an identified or identifiable natural person." The ICO interprets identifiability through the lens of **singling out**: a record is personal data if it can isolate one individual from a population, even without knowing their name (ICO — *What are identifiers and related factors?*).

Article 29 Working Party Opinion 05/2014 (WP216) sets a stricter operational test for true anonymisation. A dataset is anonymous if and only if all three of the following are defeated:

Test	Crowd-Sense wire payload
Singling out — can a record be isolated to one individual?	No. A bracket count of "12 devices in the 8–15 m ring at 14:00–14:15" identifies no individual.
Linkability — can records about the same individual be linked across datasets?	No. There is no recurring identifier of any kind to link on.
Inference — can an attribute be inferred about an individual with high confidence?	No. Population-scale bracket counts support inferences about *the place*, not about any *person*.

Recital 26 of the GDPR confirms that the principles of data protection do not apply to anonymous information — and the wire payload from a Crowd-Sense sensor is anonymous information by construction.

The on-device stage of the pipeline does briefly process personal data (a probe-request MAC may itself be personal data in some circumstances under the singling-out reading). However, that processing is conducted entirely within the sensor, lasts no longer than the longest aggregation window (60 minutes), serves the explicit purpose of producing aggregate statistics, and ends in deletion. No information about an individual ever leaves the sensor.

4. Alignment with ICO 2016 Wi-Fi Location Analytics guidance

The ICO's 2016 guidance (ICO 2016) remains the canonical UK regulatory text on this technology. It explicitly endorses aggregation as a compliance route:

> *"Remove identifiable elements by, for example, anonymising the MAC address so that individuals cannot be identified, where this would still enable a data controller to achieve the specified purpose of data collection (e.g. where the data controller's intention is to measure the number of visitors to a store, only)."*

Crowd-Sense's architecture is the strict version of that recommendation: the MAC is not "anonymised" by hashing — it is discarded entirely. We hold this is the most defensible posture under the ICO's framing.

The product is also compatible with the ICO's accompanying expectations: the controller (the venue or authority) should perform a Data Protection Impact Assessment, post visible signage at the venue boundary, and document the purpose of processing. We provide template artefacts for each (see §7).

5. What the controller is and is not responsible for

The deploying organisation is the data controller for any personal data processed in the on-device aggregation stage; Crowd-Sense is the data processor. Because the on-device processing is fully automated, time-bounded, and ends in deletion with no off-device recovery path, the controller's responsibilities are narrowly scoped:

Responsibility	Controller (venue/authority)	Crowd-Sense (processor)
Lawful basis for the on-device aggregation stage	Yes — typically Article 6(1)(e) (public task) for councils/BIDs, or Article 6(1)(f) (legitimate interest) for retailers	We assist with documentation
Data Protection Impact Assessment (Article 35 GDPR)	Yes	We supply template; we sign Article 28 processor terms
Signage / transparency at venue boundary	Yes	We supply artwork
Subject Access Requests (Article 15)	Receive and respond	We confirm in writing that no personal data exists in our systems to disclose
Right to erasure (Article 17)	Receive	The data is already deleted — typically within 60 minutes of capture, by design
Breach notification (Article 33)	Standard GDPR obligations apply	The breach surface is materially smaller than any back-end-storing alternative

A Subject Access Request directed to a Crowd-Sense deployment will be answered factually: at the time of any given request, the only personal data that ever existed about the requester (a probe-request MAC) was processed and deleted within 60 minutes of capture. There is nothing to disclose because there is nothing held.

6. How this differs from alternative approaches the controller may be reviewing

Architecture	Representative vendors	Where the privacy story strains
Hashed/salted MAC retained server-side	Cisco Spaces, Aislelabs, Meshh, Basking, Bloom Intelligence	The CNIL refused JCDecaux's pilot at La Défense in 2015 (Conseil d'État 8 Feb 2017) on the ground that a recurring salted-MAC code re-identified the same device across visits. WP216 *singling-out* and *linkability* tests fail.
Mobile SDK location-data panel	Visitor Insights, Huq, Locomizer, Placer.ai	FTC consent orders against X-Mode/Outlogic, InMarket, Mobilewalla, Gravy/Venntel (2024). Danish DPA open formal investigation into Huq. Oxfordshire County Council publicly withdrew Huq footfall figures during the Oxford congestion-charge pilot in January 2026 after a mid-2025 dataset rebalance. The consent chain depends on every partner app's lawful basis.
Camera/CV ceiling sensor	VergeSense, Xovis, Vivacity, Hoxton AI	Image processing on-device with aggregate counts emitted is broadly defensible, but image data is processed even briefly; ICO Surveillance Camera Code of Practice applies; works-council and HR-risk friction in workplaces and clinical settings.
On-device aggregation only	**Crowd-Sense (alone in surveyed market)**	**None of the above.** No back-end identifier database. No SDK consent chain. No image.

The Dutch District Court of Overijssel's February 2024 ruling overturning the Dutch DPA's €600,000 fine against the municipality of Enschede (judgment summary) is the strongest recent EU precedent: the court held that the municipality had not shown personal data was processed once anonymisation measures were applied. The reasoning supports an on-device-aggregation architecture more readily than it supports any back-end-retaining one.

7. What we provide to support DPIA sign-off

- **Architectural verification packet.** The product technical specification and the relevant firmware source components (sensor, parser, aggregator) available under NDA. The on-device deletion step is a single function call in source — verifiable by review.
- **DPIA template.** Pre-populated against the ICO accountability framework, ready for the controller's DPO to adapt and sign.
- **Signage artwork.** Compliant with ICO transparency expectations; configurable for venue or authority branding.
- **Methodology statement.** Describes the documented overcount caused by MAC randomisation (1.2–2× at 1-min windows; 2–5× at 15-min; 4–10× at 60-min) so the controller can cite the limits in its own published reporting. This is honest disclosure that no SDK aggregator or hashed-MAC vendor offers.
- **Article 28 processor terms.** Standard SCC-compatible processor agreement available on request.

References

- UK GDPR / Data Protection Act 2018; ePrivacy Directive 2002/58/EC; Privacy and Electronic Communications Regulations 2003 (PECR)
- ICO (Feb 2016), *Wi-Fi Location Analytics* — https://www.pdpjournals.com/docs/88512.pdf

- ICO, *What are identifiers and related factors?* — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/
- Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques (WP216) — https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- Conseil d'État (France), 8 February 2017 — JCDecaux La Défense WiFi pilot (decision text in English) — https://fpf.org/wp-content/uploads/2017/02/Council-of-State-Decision-Feb-2017-FPF-English-Translation.pdf
- District Court of Overijssel (Netherlands), 2 February 2024 — Municipality of Enschede WiFi-counting fine overturned (case summary) — https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_Gemeente_Enschede
- AEPD, Joint guidance on Wi-Fi tracking (May 2024)
- CJEU, Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* (19 October 2016) — on identifiability of indirect identifiers

*Document version: 2026-04-25. Crowd-Sense is a product of **Visual Solutions UK Limited** (Companies House #02955160). DPO contact: dpo@crowd-sense.com. To request the architectural verification packet under NDA, contact Jeff Burton, Director (jeff.burton@crowd-sense.com).*