SMART URBAN SENSING · PROCUREMENT RESOURCE

APC and Welfare Sensing DPIA Pack

A screening and assessment template for passenger counting and on-vehicle welfare sensing

Version 1.0 — September 2026

Prepared for completion by the controller

Smart Urban Sensing Limited
Colony, 5 Piccadilly Place, Manchester M1 3BR
sales@smarturbansensing.co.uk

What this pack contains

Important — this is a template, not legal advice

This pack is provided to support the controller's own Data Protection Impact Assessment. It is not legal advice and it is not a compliance certificate.

The operator or transport authority deploying the system is the controller. The controller determines the purposes and means of the processing, selects and justifies the lawful basis, decides retention, and owns the outcome of this assessment — including any decision that a DPIA is or is not required. Smart Urban Sensing can complete the supplier sections and provide evidence about its own system; it cannot reach those conclusions on your behalf.

Take advice from your Data Protection Officer or legal adviser before relying on any part of this document.

How to use this pack, and who does what

This pack is a working template. It is written so that a bus or shuttle operator, a local transport authority or a passenger transport executive can complete a Data Protection Impact Assessment for automatic passenger counting (APC) and, where selected, optional on-vehicle welfare sensing. The assessment logic is deliberately vendor-neutral: the screening questions, risk register and control tests apply to any APC supplier, including ours.

Some sections are pre-populated with a description of a typical counting architecture so that you are not starting from a blank page. Check every pre-populated statement against your own deployment before adopting it. Where the text says **verify**, that is an instruction, not a decoration.

Working method

1. **Assemble the facts.** Send Annex A to your APC supplier and to any CCTV or telematics supplier whose data will be in scope. Do not begin the risk analysis until the data-flow answers are in writing.
2. **Complete Step 1 (screening) first.** The screening outcome decides whether you continue to a full DPIA or stop and record a screening decision. Record the decision either way.
3. **Work through Steps 2 to 6 in order.** Describe the processing before you judge necessity, and judge necessity before you write mitigations. Mitigations written before the description tend to describe the product rather than the risk.
4. **Consult.** Involve your Data Protection Officer, operations and safety leads, and — where welfare monitoring could observe staff — trade union or staff representatives.
5. **Sign off and diarise review.** Use Step 8. A DPIA that is never revisited stops describing the system that is actually running.

Controller and processor roles

Getting the roles right at the start changes who must do what for the rest of the assessment. The table below is a starting position for a typical deployment; complete the right-hand column for your own contract and have it confirmed by your DPO and your legal or commercial team.

Party	Likely role	Typical responsibilities	Confirmed role in this deployment
Operator or transport authority	Controller	Determines purposes and means; owns the DPIA, lawful basis, retention decision, transparency and rights handling; decides whether welfare sensing is deployed.	
APC supplier	Processor	Supplies sensors, gateway, ingest, storage and dashboard; acts on documented instructions; provides data-flow, retention, security and deletion evidence.	
Hosting and broker providers	Sub-processor	Managed message broker and cloud platform; hosting location, availability and access controls must be disclosed in the sub-processor register.	
CCTV or telematics supplier	Processor (separate)	Where existing on-board CCTV or telematics is brought into scope, its own contract, retention and access rules must be assessed alongside the APC system.	
Client authority commissioning a service	Controller or joint controller	Where an authority specifies the counting purpose and receives the outputs, its role must be settled in writing rather than assumed.	

The controller owns the outcome

This pack supports your assessment; it does not replace it. Smart Urban Sensing can complete the supplier sections and evidence its own controls, but it cannot conclude on your behalf that a DPIA is unnecessary, that a lawful basis is made out, or that residual risk is acceptable. Those are controller decisions. Nothing here is legal advice; take advice from your DPO or legal adviser on anything you are unsure about.

Where the Data Protection Officer comes in

Where you have a DPO, seek their advice on the DPIA and record what they said and what you did about it — including where you departed from their advice and why. The ICO also treats a DPIA as good practice for any major project involving personal data, not only for processing that clears the high-risk threshold (ICO: how do we do a DPIA).

Documenting a decision that no DPIA is needed

If screening indicates that a DPIA is not required, that conclusion is itself a record you must be able to produce. The ICO expects the screening decision and the reasons for it to be documented (ICO: when do we need to do a DPIA). Use the screening decision box at the end of Step 1 for that purpose. Do not treat a negative screening outcome as a general finding: it applies to the configuration you screened, on the date you screened it.

Step 1 — Screening

Screening establishes whether the proposed processing is likely to result in a high risk to individuals, in which case a DPIA must be carried out **before** processing begins (UK GDPR Article 35). Answer every row. A single "Yes" in the statutory trigger block is enough to require a full DPIA.

1.1 Statutory triggers — UK GDPR Article 35(3)

Trigger	Yes	No	Evidence or reasoning
Systematic monitoring of a publicly accessible area on a large scale — for example vehicle-mounted cameras observing passengers across a fleet or a route network.			
Processing of special category data, or personal data relating to criminal convictions and offences, on a large scale — including biometric data used to identify individuals uniquely.			
Systematic and extensive automated evaluation or profiling of individuals on which decisions with significant effects are based.			

Article 35(3) is a floor, not a ceiling. ICO screening criteria also cover matters such as innovative technology, tracking of location or behaviour, processing affecting vulnerable people and combining data sets — all of which can be engaged by on-vehicle sensing (ICO screening criteria).

1.2 Practical triggers for passenger counting and welfare sensing

Question	Yes	No	Notes
Is the deployment anonymous counting only — aggregate boarding and alighting events, with no image, face template or passenger device identifier leaving the vehicle?			
Will counting data be combined with existing on-board CCTV, or will CCTV be brought into the same platform, dashboard or export?			
Will welfare or behaviour analytics be enabled (for example distress, aggression, disruption, lone-traveller or dwell signals)?			
Will any camera perform identification, face matching, demographic estimation or re-identification of individuals across journeys?			
Will counting or welfare records be linked to ticketing, smartcard, mobile app or payment records?			
Will records be linked to staff, driver, duty, rota or scheduling records, such that an individual member of staff could be identified from them?			
Will vehicle location be recorded at a granularity and frequency that could place a known individual (for example a lone passenger or a driver) at a place and time?			
Will welfare events trigger an intervention affecting a person — a driver alert, a controller dispatch, a police referral or a staff performance conversation?			

Question	Yes	No	Notes
Will any data be shared outside the controller, or hosted or supported from outside the United Kingdom?			
Does the service carry a materially higher proportion of vulnerable passengers — for example a hospital, campus, school or social-care shuttle?			

1.3 Decision rule

Anonymous counting alone. Where overhead door sensors produce only aggregate boarding and alighting counts, no image or device identifier leaves the vehicle, and the counts are not linked to any record about an individual, the processing is usually low risk and a full DPIA is usually not required. That conclusion still requires a recorded screening decision, and it still requires you to verify the "no image, no identifier" property in your own installation rather than accept it as a claim.

Anything that observes individuals. If any question in section 1.2 about CCTV, welfare analytics, identification, ticketing or staff linkage, or intervention is answered "Yes", complete a full DPIA. Observing behaviour, inferring a state such as distress or aggression, or acting on an event about a person, all move the processing away from anonymous counting.

> **A caution about the word "anonymous"**
>
> Do not describe a camera-based system as anonymous merely because no video clip is retained. Pseudonymisation is not anonymisation, and data that can still single out an individual remains personal data (ICO anonymisation guidance). The test is whether an individual can be identified or singled out, directly or indirectly, by anyone reasonably likely to try.

1.4 Screening decision record

Deployment or contract reference

Date of screening

Completed by (name and role)

DPO consulted? Date

Configuration screened (sensors, cameras, analytics, linkages, fleet size, routes)

Screening outcome — tick one: full DPIA required / DPIA not required, reasons recorded below

Reasons for the outcome, including which triggers were engaged or excluded

Signature

Review date

Step 2 — Describe the processing

Edit every paragraph and table cell below so that it describes your deployment, and delete anything that does not apply.

2.1 Purposes of the processing

Purpose	What it means in practice	In scope? Local detail
Service planning	Understanding demand by stop, hour, day and route so that timetables, frequencies and vehicle allocation match actual loadings.	
Capacity management	Identifying crowding and pass-bys, sizing vehicles, managing peak demand and informing passengers where an occupancy feed is published.	
Funding and contractual evidence	Evidencing patronage for subsidy, concessionary reimbursement, contract performance or grant reporting.	
Passenger and staff safety	Where the welfare module is enabled, raising an operational alert so that a controller or driver can respond to an incident.	
Other (specify)		

State the purposes narrowly. A broad purpose such as "operational improvement" makes function creep hard to police later, because almost any new use can be said to fall within it.

2.2 The processing chain

The chain below reflects the architecture Smart Urban Sensing deploys. Confirm each stage against your own build: the assessment must follow the chain you have.

Stage	Function	What data the stage holds
Overhead door sensors	One sensor per door. Detection and counting are performed on the device; the device outputs boarding and alighting counts.	Counts and timestamps. In the counting path, no image, face template or passenger device identifier is output by the device.
On-vehicle cellular gateway	Collects per-door counts and publishes them over MQTT secured with TLS. Carries vehicle and route identifiers.	Counts, vehicle identifier, route identifier, timestamps, position where a location source is fitted.
Managed message broker	Cloud message broker with per-client credentials and topic-level permissions.	Messages in transit; short-lived queues. No long-term passenger record.
Ingest and normalisation	Server-side service that normalises per-door topics into consistent records, applies validity and provenance rules.	Normalised count records, sensor-health state, location provenance fields.
Persistent storage	Database on a persistent volume so records survive redeploys.	Count records by stop and hour, derived aggregates, sensor-health history, welfare event records where the module is enabled, dashboard account records.
Dashboard and REST API	Daily, weekly, monthly and yearly views; route and vehicle filters; value summaries; API access for integrations.	Aggregated counts and derived metrics; welfare event states where enabled; access and diagnostic logs.
Exports and reporting	PDF, Excel and CSV exports, chart capture to PDF.	Whatever the exporting user selects. Exports leave the platform boundary and are then under the controller's own control.

2.3 Data map

Complete one row per data element. "Depends" is a legitimate answer, but resolve it before sign-off: record what it depends on and who will decide.

Data element	Source	Personal data?	Where processed	Where stored	Retention	Recipients	Confirmed
Boarding and alighting counts per door, per stop, per hour	Overhead door sensor	No — aggregate	On device, then cloud ingest	Platform database		Operator planning team	
Vehicle identifier and route identifier	Gateway config	No	Cloud ingest	Platform database		Operator, authority	

Data element	Source	Personal data?	Where processed	Where stored	Retention	Recipients	Confirmed
Vehicle position, with provenance fields recording whether the fix was measured, a stale fallback, scheduled or interpolated, or a bench-test value	Gateway or telematics	Depends — personal if linkable to a known driver or a lone passenger	Cloud ingest	Platform database and diagnostic cache		Operator, authority	
Occupancy derivation (running load)	Derived from counts	No — aggregate	Cloud	Platform database		Operator; passengers where published	
Dwell derivation — currently a proxy based on a no-alighting window, not per-passenger dwell time	Derived from counts	No — aggregate	Cloud	Platform database		Operator	
Sensor-health and liveness records, including expected shutdown windows	Ingest service	No	Cloud	Platform database		Operator, supplier support	
Welfare event records — signal, severity, zone, source, confidence score and acknowledgement. Event states are stored, not video.	On-camera analytics via an event relay	Yes, where an event concerns an identifiable person or triggers action	On camera, then cloud	Separate welfare event table		Control room, safety team	
On-board CCTV footage, where brought into scope	Existing CCTV system	Yes	On vehicle, remote viewing where enabled	CCTV recorder or CCTV supplier platform		Named reviewers, police on lawful request	
Staff dashboard accounts and access logs	Platform admin	Yes	Cloud	Platform database		Operator admins, supplier support	
Exports and reports generated by users	Dashboard	Depends on content	Cloud, then user device	Operator systems		As distributed by the operator	

A design property, not an inherent guarantee

In the counting path of the architecture described above, no image, face template or passenger device identifier leaves the vehicle. That is a property of how the sensors and the ingest chain are configured — it is not an inherent property of passenger counting, and it is not a property you should take on trust. Verify it in your deployment: inspect the device output, the broker topics and the stored record schema, and record the evidence. If a camera with image output is fitted to the same vehicle for any purpose, the statement no longer describes the vehicle as a whole.

2.4 Scale, geography and duration

Number of vehicles in scope

Number of routes or services

Estimated passenger journeys per year

Hours of operation

Geographical coverage and any services with a higher proportion of vulnerable passengers

Duration: pilot period, contract term, and the date processing is intended to start

Step 3 — Necessity and proportionality

The question here is not whether the technology works. It is whether this processing is a necessary and proportionate way to achieve the stated purpose, and whether a less intrusive option would achieve it well enough.

3.1 Alternatives considered

Option	What it gives you	Limitations	Privacy intrusion
Manual ride checks	Direct human observation; a recognised reference method and the basis for validating any automatic system.	Expensive and sampled. Cannot give continuous coverage by stop and hour across a fleet, so planning rests on extrapolation from a small sample.	Low for data protection, though a surveyor is physically present and observes passengers directly.
Ticketing-derived estimates	Uses data you already hold; no new hardware.	Systematically misses concessionary, pass, transfer and non-paying travel, and gives boardings only — not alightings, load or crowding.	Higher than it appears: ticketing records are personal data and reuse for planning raises purpose-limitation questions.
Camera-based counting with footage retention	Counts plus reviewable imagery; can be reconciled visually.	Retains images of passengers; storage, access and export controls become the dominant risk. Accuracy still requires validation.	High. Images of identifiable people, retained and potentially viewable remotely.
Anonymous overhead counting (selected)	Continuous counts by door, stop and hour across the fleet; supports planning, capacity and funding evidence.	Counts events, not people. No demographic or journey-level insight. Accuracy must still be validated per installation, and a faulty door feed degrades derived metrics.	Lowest of the options that meet the purpose: aggregate counts, with no image or device identifier leaving the vehicle in the counting path.

Why the selected option is the least intrusive that meets the purpose — controller's reasoning

Where welfare sensing is being considered, assess it as a **separate** proposal with its own purpose, its own alternatives (for example staff presence, help points, radio or driver-initiated alarms, improved lighting and layout) and its own necessity test. It should not be carried along on the necessity case for counting.

If welfare sensing is in scope: purpose, alternatives considered, and why sensing is necessary

3.2 Data minimisation and purpose limitation

- Collect counts at the lowest granularity that supports the purpose. Per-stop, per-hour aggregates usually suffice for planning; per-event records rarely add planning value and add risk.
- Keep the welfare module off unless a specific, documented safety purpose requires it, and keep it off on any vehicle with a faulty door feed where rules depend on occupancy.
- Do not enable identification, demographic estimation or re-identification features because they are available in a product.

- Where an occupancy feed is published to passengers or to an open-data service, publish a banded status rather than raw counts, and state whether the value is sensor-derived or estimated (DfT Bus Open Data Service operator requirements).

3.3 Function-creep controls

Function creep is the most predictable failure mode for on-vehicle sensing: a system installed to count passengers is later asked to answer a question about a person. Control it explicitly.

Control	How it works	Owner and status
Documented permitted-use list	A short written list of uses the system is approved for. Anything not on the list requires a change request.	
Change gate	New analytics, new linkage, new recipients or a new retention period require DPO review and a DPIA update before enablement.	
Configuration lock	Analytics features that are not approved remain disabled in configuration, and enablement is logged.	
Request log	Requests to use the data for staff performance, discipline or investigation are logged and answered against the permitted-use list.	
Contractual restriction	The processor contract prohibits use of the data for the supplier's own purposes, including model training, without written instruction.	

3.4 Accuracy, and why it is a fairness question

Accuracy is a data protection principle, not only an engineering metric. A wrong count drives a wrong service decision: an undercount can justify withdrawing or thinning a service that people depend on, and an overcount can hide crowding that affects safety and comfort. Where the service in question is a hospital, campus or social-care shuttle, the people affected by a wrong decision are often those with fewest alternatives.

- Validate accuracy per installation against manual reference counts, and record the result per door and per route rather than adopting a single headline percentage.
- Require the supplier to state the denominator (boardings, alightings or occupancy), the sample, the vehicle, door, sensor and firmware scope, the matching rules and the confidence interval. VDV-Schrift 457 sets out a statistical framework for this (VDV 457 current version page).
- Re-validate after firmware or sensor changes that could affect the count core, and periodically thereafter.
- Treat sensor health as part of accuracy. Feed-liveness thresholds, expiry of stale positions and suppression of derived alerts on untrusted data all prevent a broken feed from being read as a real observation.
- Publish the caveats alongside the numbers when count data is used in a funding or service-withdrawal case, so that decision-makers know the confidence attached.

Accuracy validation plan: method, reference counts, tolerance, dates, who signs off

3.5 Storage limitation

Set a retention period for each data class, tie it to the purpose, and make deletion automatic rather than a task someone must remember. Annex B gives the fuller schedule; the table below records the headline decisions.

Data class	Retention	Justification tied to purpose	Deletion mechanism and evidence
Raw per-event count messages		Only needed until aggregation and validation are complete.	
Aggregated counts by stop and hour		Planning, funding and trend comparison over multiple years.	

Data class	Retention	Justification tied to purpose	Deletion mechanism and evidence
Sensor-health and diagnostic records		Fault investigation and data-trust assurance.	
Location records and provenance fields		Route attribution and data-quality investigation.	
Welfare event records		Incident response, review of false-alarm rate, and any consequential investigation.	
CCTV footage, where in scope		Incident investigation only; normally days, not months.	
Access, audit and login logs		Security monitoring and accountability.	
Exports held by the operator		Controlled by the operator once exported.	

3.6 Transparency

Step 7 provides model wording. Record here how it will actually reach people: on-vehicle notices at the doors, a privacy notice section on your website, staff briefing and, where welfare monitoring affects drivers, consultation and written notification.

Transparency measures, locations and dates

Step 4 — Lawful basis

A lawful basis is only needed where personal data is processed. If, after Step 2, you are satisfied that the counting outputs are genuinely aggregate and cannot single out an individual, record that reasoning and note that UK GDPR does not apply to that data. Be conservative: if any element of the deployment processes personal data — welfare events, location that can be tied to a driver, CCTV, staff accounts — identify a basis for each of those elements.

4.1 Choosing a basis

Basis	Who it typically suits	What you must be able to show	Selected?
Public task — Article 6(1)(e)	Local transport authorities, passenger transport executives, and other public authorities carrying out their transport functions.	A task, function or power laid down in law, and that the processing is necessary for it. The basis is not automatic merely because you are a public body (ICO public task guidance).	
Legitimate interests — Article 6(1)(f)	Commercial bus and shuttle operators, including campus and healthcare shuttle operators.	A documented legitimate interests assessment covering purpose, necessity and balancing, including passengers' reasonable expectations (ICO legitimate interests guidance).	
Legal obligation — Article 6(1)(c)	Rarely the basis for counting itself; may apply to specific reporting duties.	The obligation, and that the processing is necessary to comply with it.	
Consent — Article 6(1)(a)	Not recommended for this processing.	Freely given, specific, informed and unambiguous consent, capable of being withdrawn without detriment.	

4.2 Why consent does not work at a bus door

Consent must be a real choice. A passenger boarding a bus cannot meaningfully agree or refuse at the door: there is no opportunity to read a notice and decide before the sensor above the door registers the boarding, refusal would mean not travelling, and there is no practical mechanism to count some passengers and not others. Relying on consent here would also produce an incomplete data set, which undermines the planning purpose. Neither is

contractual necessity a shortcut: carrying a passenger does not require counting them, still less observing their behaviour.

4.3 Legitimate interests assessment (commercial operators)

Complete all three parts. A legitimate interests assessment that records only the benefit to the operator has not done the balancing.

Part 1 — Purpose test

What is the legitimate interest? Who benefits, and how substantial is the benefit?

Part 2 — Necessity test

Why is this processing necessary to achieve that interest? What less intrusive means were rejected, and why?

Part 3 — Balancing test

Consideration	Assessment
Nature of the data — aggregate counts, location, behavioural inference, images	
Reasonable expectations of passengers — would a reasonable passenger expect counting? Would they expect behavioural analysis?	
Reasonable expectations of staff, where the sensing could observe drivers	
Possible impact on individuals — intrusion, chilling effect, wrongful intervention, consequences of an inaccurate record	
Vulnerable individuals — children, patients, disabled passengers, lone travellers	
Safeguards applied — minimisation, on-device processing, retention limits, access control, suppression of alerts on untrusted data	
Conclusion — does the interest outweigh the effect on individuals, and on what reasoning?	

Completed by

Date

DPO comment

Outcome

4.4 Special category and biometric processing

"Biometric data" is defined in UK GDPR Article 4, and biometric data processed for the purpose of uniquely identifying a person is special category data under UK GDPR Article 9. If any part of the deployment processes facial images or other characteristics for identification, you must identify an Article 9 condition as well as an Article 6 basis, and the risk assessment must be correspondingly deeper. Health inferences drawn from a welfare signal can also be special category data even where no camera identifies anyone.

Question	Yes/No	If yes: Article 9 condition, safeguards and policy document
Does the system process biometric data for the purpose of unique identification?		

Question	Yes/No	If yes: Article 9 condition, safeguards and policy document
Could a welfare signal amount to an inference about a person's health?		
Could any output relate to criminal offences or suspected offences?		

4.5 Anonymisation versus pseudonymisation

Irreversibly aggregated counts that cannot identify or single out a person fall outside UK GDPR. Replacing an identifier with a reference, or retaining data from which an individual could still be singled out, is pseudonymisation — and pseudonymised data is still personal data (ICO anonymisation guidance). Two practical consequences follow. First, do not call a camera-based system anonymous because no clip is retained: the question is what the system can single out, not what it keeps. Second, record the reasoning behind any "not personal data" conclusion, including who might reasonably be able to re-identify and with what other data sets, so that the conclusion can be re-tested when the deployment changes.

> **ICO guidance is being updated**
>
> The Data (Use and Access) Act 2025 amended UK data protection law and ICO guidance is being revised in consequence (ICO DPIA guidance hub). Do not rely on pre-2025 summaries of DPIA or lawful-basis requirements. Confirm the current position with your DPO at the point of decision.

Step 5 — Risk register

Score each risk before mitigation, record the mitigation, then score the residual risk. Likelihood and severity use a three-point scale: Low, Medium, High. Overall risk is the higher of the two unless you record a reason to depart from that. Any residual risk that remains High must be escalated under Step 8 and may require prior consultation with the Information Commissioner's Office.

ID	Risk	Affected	Like.	Sev.	Overall	Mitigation	Resid.	Owner
R1	Re-identification by joining data sets — counts, location and timing combined with ticketing, rota or CCTV data allow an individual journey to be reconstructed.	Passengers and staff	Med	High	High	Prohibit joins that are not on the permitted-use list; keep counting data in a separate store from ticketing; hold aggregates rather than per-event records; test re-identification risk on low-patronage services where a single boarding may be one known person.	Med	DPO
R2	Function creep — a counting system is progressively used for surveillance, staff monitoring or investigation.	Passengers and drivers	High	High	High	Written permitted-use list; change gate requiring DPO review and a DPIA update; unapproved analytics disabled in configuration with enablement logged; contractual restriction on supplier use; request log reviewed periodically.	Low	Head of Operations
R3	Retention drift — data is kept because deletion was never automated, so records accumulate well beyond the period the purpose justifies.	Passengers and staff	High	Med	High	Retention periods configured in the platform rather than managed by hand; scheduled deletion jobs; periodic retention audit with evidence of deletion; retention change treated as a DPIA review trigger.	Low	Data owner

ID	Risk	Affected	Like.	Sev.	Overall	Mitigation	Resid.	Owner
R4	Excessive access through shared dashboard credentials — access cannot be attributed to a person and leavers retain access.	Passengers and staff	High	Med	High	Move to per-user accounts with role-based access and login auditing; rotate all shared credentials before go-live and remove them from any shared document; maintain a named access list reviewed on a fixed cycle; joiner-mover-leaver process.	Low	IT and platform owner
R5	Credentials exposed in code or in client-side assets — broker or API secrets are committed to a repository or shipped to the browser.	Passengers, staff and operator	Med	High	High	Secrets held in environment configuration, never in source or client-side code; secret scanning on the repository; rotation on any suspected exposure; server-side proxying of any API call that needs a secret.	Low	Supplier engineering lead
R6	Broker over-permissioning — one client credential can subscribe to all topics across the fleet or publish spoofed data.	Passengers and operator	Med	High	High	Per-client credentials with topic-scoped, least-privilege permissions; separate credentials per vehicle and per environment; TLS enforced; periodic review of broker access control lists.	Low	Supplier engineering lead
R7	False welfare alerts causing wrongful intervention — a person is approached, challenged or reported on the basis of an incorrect event.	Passengers	High	High	High	Treat welfare output as a prompt for human judgement, never an automatic decision; confidence score and zone shown with every event; acknowledgement workflow with a recorded outcome; repeat-event cooldown; documented false-alarm rate from a moving-vehicle acceptance trial before fleet enablement; staff training on proportionate response.	Med	Safety lead
R8	Welfare analytics misclassify behaviour — loud conversation, disability-related movement or distress are mislabelled as aggression, with unequal impact across groups.	Passengers, especially disabled and minority passengers	Med	High	High	Do not publish or act on classification as fact; review event outcomes for patterns of misclassification; keep human review in the loop; suppress rules where sensor conditions are poor; equality impact review alongside this DPIA.	Med	DPO and safety lead
R9	Inaccurate counts drive service withdrawal — an undercount removes a service that dependent passengers rely on.	Passengers without alternatives	Med	High	High	Per-installation validation against manual reference counts recorded per door and per route; no single headline accuracy figure used in decisions; confidence and exclusions published with the data; re-validation after firmware or sensor change; service-change decisions require a data-quality statement.	Low	Planning lead

ID	Risk	Affected	Like.	Sev.	Overall	Mitigation	Resid.	Owner
R10	Stale or fabricated-looking location data misrepresents where a vehicle — and therefore a person — was at a given time.	Drivers and passengers	Med	High	High	Provenance fields on every location record distinguishing measured, stale-fallback, scheduled or interpolated and bench-test values; stale positions expire rather than being presented as current; diagnostics persisted so the provenance of a historical record can be reconstructed; no disciplinary or evidential use of a record without a measured fix.	Low	Supplier engineering lead
R11	Transfer or hosting outside the United Kingdom — data, backups or remote support sit outside the UK without a transfer mechanism.	Passengers and staff	Med	Med	Med	Document hosting, backup and support locations in the sub-processor register; contractual transfer mechanism and transfer risk assessment where applicable; restrict support access to named individuals with logged, time-limited sessions.	Low	DPO and commercial lead
R12	Supplier or sub-processor change made without assessment — a new hosting provider, broker or analytics component is introduced silently.	Passengers and staff	Med	Med	Med	Contractual notice and objection rights for sub-processor change; maintained sub-processor register; change treated as a DPIA review trigger; exit and data-return or deletion terms agreed at contract, with evidence of deletion.	Low	Commercial lead
R13	Loss of availability hides an outage — a silent sensor or gateway makes a vehicle appear empty rather than unmonitored, corrupting the planning picture.	Passengers and operator	High	Med	High	Feed-liveness thresholds with explicit stale and offline states; known fleet seeded so a silent vehicle cannot drop out of the coverage denominator; scheduled shutdowns classified as expected rather than as faults; derived alerts suppressed on untrusted data; outage visible on the dashboard and in exports.	Low	Supplier support
R14	Passengers and staff unaware of the processing — no notice, or notice that does not describe what is actually happening.	Passengers and drivers	Med	Med	Med	On-vehicle notices at each door; privacy notice section published and dated; notice text reviewed whenever analytics change; staff briefing and, where welfare monitoring affects drivers, consultation with staff representatives.	Low	Comms lead

Scores shown are an illustrative starting position drawn from typical deployments. Re-score every row for your own fleet, service mix and control environment, and add any risk specific to your operation. Add rows as needed.

Additional risks identified locally

Step 6 — Measures and controls

Record the technical and organisational measures you rely on, which risks each one addresses, and — importantly — the evidence that the measure is actually in place. A control that exists only in a product description does not reduce residual risk.

6.1 Technical measures

Measure	What it does	Risks	Evidence and status
On-device counting	Detection and counting occur on the sensor; only counts leave the device, so no image or device identifier enters the data chain in the counting path. Verify in the specific installation.	R1, R2	
Event-only welfare output	Camera analytics run on the camera; a relay ignores clear states, applies a repeat cooldown and posts normalised event states — signal, severity, zone, source, confidence, acknowledgement — rather than video.	R7, R8	
TLS in transit	All telemetry published over MQTT secured with TLS; API and dashboard traffic over HTTPS.	R5, R6	
Per-client broker credentials, least privilege	Each vehicle and each environment holds its own credential with topic-scoped permissions, so one compromise does not expose the fleet.	R6	
Credential rotation and secret hygiene	Broker and dashboard credentials removed from code, rotated before go-live and on suspicion of exposure; secrets held in environment configuration.	R4, R5	
Environment isolation	Development and welfare-module work run on separate services, databases, volumes and broker client identifiers, so new development cannot displace or corrupt production.	R12, R13	
Health-gated releases	A health endpoint gates deployment; a failed validation leaves the previous working release serving.	R13	
Persistent audit and diagnostic trail	Diagnostic state is held on a persistent volume so it survives restarts and the provenance of a historical record can be reconstructed.	R10, R13	
Provenance fields on location records	Every position carries validity and source fields distinguishing measured, stale-fallback, scheduled or interpolated and bench-test values.	R10	
Feed-liveness thresholds	Defined stale and offline thresholds, with the known fleet seeded so a silent vehicle remains visible in the coverage denominator.	R13	
Suppression of derived alerts on untrusted data	Welfare and occupancy-gated rules are suppressed where the underlying passenger data is unreliable or a door feed is faulty.	R7, R8, R13	
Retention enforcement	Retention periods configured and enforced by scheduled deletion, with deletion evidence available on request.	R3	
Access control and logging	Role-based access, named accounts and login auditing, with access logs retained for review. Note the roadmap position in the closing section of this pack.	R4	

6.2 Organisational measures

Measure	Requirement	Owner, date and evidence
Processor contract	Article 28 terms in place, including processing only on documented instructions, confidentiality, security, sub-processor controls, assistance with rights and DPIAs, and deletion or return at the end of the contract.	
Sub-processor register	Maintained list of sub-processors with function, hosting location and notice arrangements for change.	
Permitted-use list and change gate	Written approved uses; DPO review before any new analytics, linkage, recipient or retention change.	
Incident response and breach notification	Defined detection, triage and escalation route. Processor notifies the controller without undue delay; the controller assesses whether the incident must be reported to the ICO within 72 hours of becoming aware, and whether affected individuals must be told.	
Rights and DSAR handling	Documented procedure with a defined supplier assistance time, including the position where no identifier is held: explain what is and is not held, search the data classes that could relate to the requester (welfare events, CCTV, staff accounts), and record the search performed rather than issuing a bare denial.	
Training and briefing	Role-appropriate training for dashboard users, control-room staff and drivers, covering permitted use, proportionate response to welfare events and reporting of suspected incidents.	
Security assurance	Proportionate assurance requested from the supplier — security questionnaire, architecture and data-flow, vulnerability and patch process, access logging, backup and business continuity. Certification such as Cyber Essentials or an certificated information security management system may be required where proportionate, but only against a current certificate in the supplier entity's name and with a stated scope.	
Accessibility and equality review	Installation survey confirming sensors, brackets and cabling do not obstruct wheelchair or priority space, gangways, handrails or boarding equipment; equality impact review where behavioural analytics are enabled.	
Periodic audit	Scheduled review of access lists, retention compliance, sub-processors, accuracy validation and welfare false-alarm rate.	

Step 7 — Transparency

The wording below is a model an operator can adapt. Keep it short and in plain English, put it where people will actually see it, and make sure it describes what the system really does. A notice that overstates or understates the processing is worse than no notice, because it misleads.

7.1 On-vehicle notice — anonymous counting only

Model notice text (adapt the bracketed items)

PASSENGER COUNTING IN USE

Sensors above the doors count how many people get on and off. They do not take photographs or video, do not record faces, and do not identify you or your phone. We use the counts to plan services and manage capacity.

More information: [operator website address]. Questions: [contact address].

7.2 On-vehicle notice — welfare analytics or CCTV in scope

Model notice text (adapt the bracketed items)

CCTV AND SAFETY MONITORING IN USE

[Operator name] operates cameras on this vehicle for the safety of passengers and staff, and sensors that count how many people get on and off.

The cameras [record images / analyse events on board] and can raise an alert to our control room about [describe: for example a fall, aggression or a raised-voice event]. An alert is reviewed by a person before any action is taken.

Footage and alert records are kept for [period] and are only seen by authorised staff, or shared where the law requires it.

Full privacy notice: [web address]. Data protection contact: [address]. You have rights over your personal data, including the right to ask for a copy.

Signage should be legible from the boarding position, placed at each door where counting occurs and near cameras where imagery is captured. ICO video surveillance guidance sets out expectations for signage, transparency and access controls where imagery is processed (ICO CCTV and video surveillance guidance). The 2021 Surveillance Camera Code of Practice is also relevant context, particularly for local authorities (Home Office update to the Surveillance Camera Code).

7.3 Privacy notice section — model wording

Heading	Model wording to adapt
What we collect	Counts of passengers boarding and alighting at each stop, the vehicle and route, the time, and the vehicle's location. [Where welfare sensing is enabled: records of safety events detected on board, including the type of event, its severity, where on the vehicle it occurred and whether staff acknowledged it.]
What we do not collect	In our passenger counting system, no images, face templates or phone identifiers leave the vehicle. [Delete or amend if CCTV or camera analytics are in use, and describe those separately.]
Why we collect it	To plan and manage services, match capacity to demand, evidence patronage for funding and contracts, and [where applicable] respond to safety incidents on board.
Our lawful basis	[Public task under Article 6(1)(e) of the UK GDPR, because [function laid down in law] / Legitimate interests under Article 6(1)(f), because [interest], and we have carried out a legitimate interests assessment which you can request.]
How long we keep it	[Data class: period] — see our retention schedule. We delete data automatically at the end of the period.
Who we share it with	[Our technology supplier acting on our instructions, its hosting and messaging providers, and [authority name] for service planning. We share with the police or other authorities only where the law allows or requires it.]
Your rights	You have the right to ask for a copy of your personal data, to have inaccurate data corrected, to object to or restrict processing, and to complain to the Information Commissioner's Office. Where our counting data holds nothing that identifies you, we will tell you that and explain what we searched.
Contact	[Data protection contact name, postal address and email address. DPO details where one is appointed.]

Step 8 — Consultation, residual risk and sign-off

8.1 Consultation

Who	Why	Consulted? Date and outcome
Data Protection Officer	Statutory advice on the DPIA, lawful basis, retention and residual risk. Record the advice and the response to it.	
Safety and operations leads	Whether the alerting workflow is deliverable and proportionate, and who will respond to events.	

Who	Why	Consulted? Date and outcome
Trade union or staff representatives	Required where welfare or behavioural monitoring could observe drivers or other staff. Consult before enablement, not after.	
Passenger representatives or user groups	Whether the processing matches passenger expectations and whether the notice wording is understood.	
Accessibility advisers	Installation effects on wheelchair and priority space, gangways and boarding equipment; effects of behavioural analytics on disabled passengers.	
Information security	Access control, credential management, broker permissions and incident response.	
Commissioning authority, where applicable	Controller roles, data sharing and reporting obligations.	
Processors and sub-processors	Accuracy of the data-flow description, hosting locations, retention capability and deletion evidence.	

8.2 Residual risk and acceptance

Summary of residual risks after mitigation, including any scored High

Residual-risk acceptance statement

I confirm that the risks identified in this assessment have been evaluated, that the measures recorded in Step 6 are in place or scheduled with named owners and dates, and that the residual risk is accepted by [controller name] for the processing described in Step 2. Where any residual risk remains High and cannot be reduced, processing will not begin until the Information Commissioner's Office has been consulted in accordance with the prior consultation requirement in UK GDPR Article 35.

Question	Yes/No	Reasoning and next step
Does any residual risk remain High?		
Is prior consultation with the ICO required before processing begins?		
Has consultation been requested? Reference and date		

8.3 Sign-off

Role	Name	Signature	Date
Assessment completed by			
Data Protection Officer — advice given			
Information security owner			
Operations or safety owner			
Senior responsible owner — risk accepted			
Commissioning authority, where applicable			

DPIA version and reference

Scheduled review date

8.4 Review and reassessment triggers

Review this assessment on the scheduled date and, in any event, whenever one of the following occurs. Record the trigger, the date and the outcome.

Trigger	Trigger occurred: date, description and outcome
New analytics or signals enabled, including any camera-based feature	
New data sharing, new recipient or a new linkage to another data set	
Change to a retention period or to the deletion mechanism	
Supplier, sub-processor, hosting location or broker change	
Fleet expansion, new route type, or extension to a service with more vulnerable passengers	
Security incident, personal data breach, or a near miss	
Material accuracy problem, extended outage or a systematic sensor fault	
Complaint, rights request or regulatory enquiry that reveals a gap	
Change in law or in ICO guidance, including guidance revised following the Data (Use and Access) Act 2025	

Annex A — Supplier information request

Send this to the APC supplier and to any CCTV or telematics supplier whose data will be in scope. Ask for written answers with evidence attached, and treat "commercially confidential" as a reason to sign a non-disclosure agreement rather than a reason to accept a gap. A supplier can and should provide DPIA inputs; it cannot conclude that a DPIA is unnecessary.

#	Question	Supplier response and evidence attached
A1	Provide a complete data-flow diagram from sensor to storage to export, naming every component and protocol.	
A2	List every data element the system holds at each stage, and state which are personal data in your view and why.	
A3	Confirm what leaves the vehicle in the counting path. State explicitly whether any image, video frame, face template or device identifier is transmitted, and how we can verify this in our own installation.	
A4	Where welfare or behavioural analytics are offered, state what is processed on the device, what is transmitted, what is stored, and whether any imagery is retained.	
A5	List all hosting, processing, backup and support locations by country, including any remote access from outside the United Kingdom.	
A6	Provide your sub-processor register with function and location, and your notice and objection terms for change.	
A7	State the retention periods the platform can enforce per data class, whether they are configurable by us, and how deletion is executed.	
A8	Describe how you evidence deletion, and provide a sample deletion report.	
A9	Describe access controls: authentication model, per-user accounts, role-based permissions, login auditing, session management and administrative access by your own staff.	
A10	Describe credential management for the message broker and dashboard, including per-client permissions, rotation policy and how secrets are kept out of source code.	
A12	Provide security certifications with the exact legal entity, scope and expiry date, or explain what assurance you offer instead.	
A13	State your breach notification terms: detection, the time within which you will notify us, what information you will provide, and your support during our own assessment.	
A14	Describe your accuracy validation method, and provide validation results for installations comparable to ours, including denominator, sample, tolerance, vehicle, door, sensor and firmware scope.	
A15	Describe sensor-health monitoring, liveness thresholds and how an outage is made visible in the data rather than appearing as zero demand.	
A16	Describe location data provenance: what fields record measurement validity and source, and how stale positions are prevented from appearing as current.	
A17	Confirm whether you use any of our data for your own purposes, including product development, benchmarking or model training, and on what basis.	
A18	Describe your assistance with rights requests, including the position where no identifier is held, and your response times.	
A19	Describe exit arrangements: data return format, deletion timetable and evidence, and transition support.	

#	Question	Supplier response and evidence attached
A20	List any features that are pilot-stage, in development or not yet validated in a moving vehicle, and state what would be required before we could rely on them.	

Annex B — Retention schedule template

Complete one row per data class. The justification must connect the period to the purpose in Step 2.1; "in case it is useful" is not a justification. Where the platform cannot enforce a period automatically, record the manual control and who performs it.

Data class	Retention period	Justification linked to purpose	Deletion method	Automated or manual	Owner
Raw per-event count messages					
Normalised count records					
Aggregated counts by stop and hour					
Occupancy and dwell derivations					
Vehicle location records and provenance fields					
Sensor-health and liveness records					
Welfare event records					
On-board CCTV footage, where in scope					
Dashboard user accounts					
Access, login and audit logs					
Support and diagnostic logs held by the supplier					
Exports and reports held by the operator					
Rights request records					
Backups					

Schedule approved by

Date

Next retention audit due

Evidence of last deletion run

Annex C — Sources

Every legal instrument and guidance page relied on in this pack is listed below with its issuing body and full address. Verify the current version at the point of use: legislation and guidance both change, and a template cannot keep pace with them.

#	Instrument or guidance	Issuing body	Address
1	**UK GDPR Article 35 — Data protection impact assessment**	Legislation.gov.uk (retained EU law)	https://www.legislation.gov.uk/eur/2016/679/article/35
2	**UK GDPR Article 4 — Definitions (including biometric data)**	Legislation.gov.uk (retained EU law)	https://www.legislation.gov.uk/eur/2016/679/article/4
3	**UK GDPR Article 9 — Processing of special categories of personal data**	Legislation.gov.uk (retained EU law)	https://www.legislation.gov.uk/eur/2016/679/article/9
4	**When do we need to do a DPIA?**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/
5	**How do we do a DPIA?**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/
6	**Data protection impact assessments (DPIAs) — guidance hub and update status**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
7	**CCTV and video surveillance guidance**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/
8	**Lawful basis: public task**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/public-task/
9	**Lawful basis: legitimate interests**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/
10	**Anonymisation guidance (anonymisation and pseudonymisation)**	Information Commissioner's Office	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/
11	**Data (Use and Access) Act 2025**	Legislation.gov.uk / UK Parliament	https://www.legislation.gov.uk/ukpga/2025/18/contents
12	**Update to the Surveillance Camera Code of Practice (2021 code)**	Home Office / GOV.UK	https://www.gov.uk/government/publications/update-to-surveillance-camera-code
13	**Surveillance Camera Code of Practice (2013 publication — WITHDRAWN)**	Home Office / GOV.UK	https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
14	**Protection of Freedoms Act 2012, Part 2 Chapter 1 (ss.29–36)**	Legislation.gov.uk	https://www.legislation.gov.uk/ukpga/2012/9/part/2/chapter/1
15	**VDV-Schrift 457 — Automatic passenger counting systems (current version page)**	Verband Deutscher Verkehrsunternehmen (VDV)	https://www.vdv.de/afzs.aspx
16	**VDV Recommendation 457 v2.1 (04/2018), published English text**	Verband Deutscher Verkehrsunternehmen (VDV)	https://www.vdv.de/457-v2.1-ses.pdfx
17	**Bus Open Data Service — operator requirements (bus location profile)**	Department for Transport	https://publish.bus-data.dft.gov.uk/guidance/operator-requirements/?section=buslocation
18	**The Public Service Vehicles (Open Data) (England) Regulations 2020 (SI 2020/749)**	Legislation.gov.uk	https://www.legislation.gov.uk/uksi/2020/749/contents
19	**ISO/IEC 27001 — information security management (overview)**	International Organization for Standardization	https://www.iso.org/isoiec-27001-information-security.html
20	**Cyber Essentials — overview**	National Cyber Security Centre	https://www.ncsc.gov.uk/cyberessentials/overview

Two status caveats that matter for this pack

Data (Use and Access) Act 2025

The Data (Use and Access) Act 2025 amended UK data protection law, and the ICO has stated that its guidance is being updated in consequence. Pre-2025 summaries of DPIA obligations, lawful basis or rights handling — including third-party articles and older internal templates — should not be relied on for a conclusion. Confirm the current position from the revised legislation and the ICO's updated guidance, and take your DPO's view at the point of decision. On the primary sources checked for this pack, no provision was verified that repeals the Protection of Freedoms Act 2012 surveillance-camera code framework.

Surveillance Camera Code of Practice

The revised Surveillance Camera Code of Practice was laid under section 31(3) of the Protection of Freedoms Act 2012 on 16 November 2021 and came into force on 12 January 2022. The statutory framework in sections 29 to 36 of that Act remains in force as revised legislation. The code is directed chiefly at police forces and local authorities in England and Wales rather than at commercial operators generally, and it is guidance rather than a product certification. The earlier 2013 GOV.UK publication of the code is marked withdrawn and should not be cited as current.

How Smart Urban Sensing supports your DPIA

We publish this pack because a good DPIA makes for a better deployment, and because the questions in it are the questions we would want asked of any supplier, including us. The assessment is yours. What we can do is make the inputs to it reliable.

What we provide	What it contains
Completed supplier sections	Annex A answered in writing for your specific configuration, with evidence attached, so your DPIA rests on documented fact rather than on a brochure.
Data-flow documentation	A component-level diagram from sensor to export, the data held at each stage, and the verification steps you can run yourself to confirm what does and does not leave the vehicle.
Retention configuration	Retention periods configured per data class to your schedule, with deletion enforced automatically and deletion evidence available on request.
Accuracy validation support	A per-installation validation against manual reference counts, with the result recorded per door and per route, and re-validation after changes affecting the count core.
Integrity and health evidence	Location provenance fields, feed-liveness thresholds and suppression of derived alerts on untrusted data, so your data-quality assumptions can be tested rather than assumed.
Security and access artefacts	Per-client broker credentials with least-privilege permissions, credential rotation before go-live, environment isolation and health-gated releases, with the sub-processor register supplied.

Where we draw the line — scope and limits, stated openly

Welfare signals are commissioned per fleet. Detection runs on the camera in the vehicle, and classification, deduplication, storage and acknowledgement are built and in service; thresholds were calibrated by replaying real service history. The acceptance test — covering vibration, braking, HVAC noise, changing light, cellular gaps and false-alarm rate — is carried out on the controller's own vehicles before the signals go live to a control room, and the camera holds no vehicle-specific certification for this application.

The dwell signal is currently a proxy based on a no-alighting window, not per-passenger dwell time. Native sensor dwell fields require validation before any direct dwell claim is made.

Per-user authentication with role-based administration and login auditing is a roadmap item. Dashboard access today uses a shared credential, which is why credential rotation and hardening are treated as pre-deployment work in Step 6 and why R4 in the risk register is scored as it is.

We claim no certification without a current, scoped audit certificate in our legal entity's name. Where a tender requires certification we will say plainly whether we hold it.

Reference deployment

The architecture described in this pack is in daily production service with a US healthcare-campus shuttle operation, where the counting path, sensor-health rules and location provenance fields have been exercised on a live feed. Operator identity, fleet size and route detail are kept confidential. Welfare signals were calibrated against replayed service history from that deployment and are commissioned on the controller's vehicles as described above.

Contact

Contact	Detail
Company	Smart Urban Sensing Limited
Registered office / studio	Colony, 5 Piccadilly Place, Manchester M1 3BR
Enquiries	sales@smarturbansensing.co.uk
Ask us for	Completed Annex A, data-flow documentation, retention configuration and accuracy validation plan for your fleet.
Document	APC and Welfare Sensing DPIA Pack — Version 1.0 — September 2026

This document is provided for information and template use. It is not legal advice, and it does not certify compliance for any operator or authority.