

APC Specification Checklist

A buyer's requirement checklist for automatic passenger counting tenders

Version 1.0 — September 2026

A supplier-neutral requirements checklist for automatic passenger counting (APC) and on-vehicle sensing. Written so that a UK bus operator, local transport authority or PTE can paste the requirement wording straight into an invitation to tender, score the responses consistently, and ask for the evidence that turns a supplier assertion into a verifiable fact. It is deliberately written so that it can be used against Smart Urban Sensing itself; where we do not yet meet a line, we say so on the closing page.

What this document is

Ten scoreable requirement sections covering accuracy and validation, sensors and vehicle fit, gateway and connectivity, data platform and storage, data quality and observability, integration and open data, security, privacy and data protection, reporting, and commercial and support terms. Each row states the requirement, why it matters, and the evidence to request — with a blank score column. It closes with ten vendor claims to challenge, a scoring summary sheet and a fully referenced source list.

Smart Urban Sensing Limited

Colony, 5 Piccadilly Place, Manchester M1 3BR

sales@smarturbansensing.co.uk

This document is guidance for procurement teams and is not legal advice. Confirm data-protection and type-approval conclusions with your own DPO and vehicle engineering function.

How to use this checklist

Scoring, weighting, and why an unevidenced “yes” must not be scored as compliance.

Who this is for

Procurement, engineering, data and DPO functions in bus operators, local transport authorities, PTEs and campus or healthcare shuttle operations buying automatic passenger counting, occupancy reporting or wider on-vehicle sensing. Every row is written as a demand the buyer makes, not as a description of a product.

How to use it

Copy the Requirement column into your specification, keep the Evidence to request column as the response instruction, and keep the Why it matters column for your internal evaluation guidance or your moderation record. Delete rows that do not apply to your scope rather than leaving them unscored – an unscored row invites a bidder to skip it. The Score column is intentionally blank.

Scoring scale

Score each row 0–3. 0 = not evidenced: no answer, or an answer that restates the question. 1 = asserted: the bidder says yes but supplies nothing a third party could check. 2 = evidenced: the bidder supplies its own artefact – a test report, sample dataset, architecture diagram, policy, screenshot or configuration extract – that is specific to the offered product and version. 3 = independently verified: the evidence is a certificate, type approval, test-house report, accredited audit or a validation signed off by a party independent of the bidder, in the name of the legal entity that will hold the contract, and current at the date of the tender.

A “yes” without evidence is not a yes

The most common failure mode in APC procurement is scoring a confident tick-box as compliance. If a bidder answers “yes” to accuracy, certification, open-data or privacy rows without an attached artefact, score 1 and say so in your moderation notes. Where a bidder cites a standard, check that the named legal entity, the named product, the version and the scope all match the offered solution; a certificate held by a parent company, an earlier hardware revision or a different subsidiary is not evidence for this contract.

Weighting the sections

Weight to the risk you are actually carrying. A suggested starting split for a fleet-wide APC contract used for service planning and funding evidence: Accuracy and validation 25%, Data quality and observability 10%, Integration and open data 10%, Data platform and storage 10%, Security 10%, Privacy and data protection 10%, Sensors and vehicle fit 8%, Gateway, connectivity and resilience 7%, Reporting and usability 5%, Commercial, delivery and support 5%. If the data will be used for revenue sharing or statutory returns, raise

Accuracy to 30–35% and set a minimum pass mark on section A rather than allowing a strong commercial score to compensate.

Minimum pass marks

Set explicit gates as well as weights. A workable pattern: any row scored 0 in sections A, G or H triggers a clarification round; a mean score below 2 in section A is a fail regardless of total; and no award without a written validation plan (section A) and a signed vehicle-fit assurance (section B).

Pilot before fleet

Treat the tender as buying a validated pilot first and a fleet rollout second. Most rows in this checklist can only reach score 3 after installation on your vehicles, so make acceptance of the fleet stage conditional on the pilot evidence rather than on the bid document.

Standards caution

Standards named in this checklist are cited from the sources listed on the Sources page, with the version and issuing body stated. Several relevant documents are licensed or paywalled: where a numerical threshold is quoted here it is quoted from the publicly available text and labelled as such. Require the bidder to work to the current licensed text and to state where its evidence differs from the published figures.

The rule that saves the most money

Score the evidence, not the answer. Where a bidder cannot supply an artefact, the honest score is 1 — and a bidder that says so plainly is usually a lower risk than one that claims 3 and cannot produce the certificate.

Section A — Accuracy and validation

The single most important section. An accuracy percentage with no stated method, denominator or sample is not procurement-grade evidence [S1][S3][S13]. Everything here is about making the bidder show the method.

Ref	Requirement	Why it matters	Evidence to request	Score
A1	The supplier shall state the accuracy claim as a method, not a number: define the measured quantity (boardings, alightings, occupancy), the denominator, the population of stop-door events, the vehicle, door, sensor and firmware coverage, the exclusion rules and the date of the measurement.	"99% accurate" is untestable without a denominator and a population. Two suppliers can quote the same figure from wholly different methods.	Written accuracy statement in the form: metric, denominator, sample, coverage, confidence interval, exclusions, date. Reject a bare percentage.	
A2	Validation shall be against manual reference counts collected on complete journeys, counting boarders, alighters and, where practicable, occupancy, with complete, traceable and tamper-proof records retained.	Manual reference counting is the recognised comparison basis in VDV-Schrift 457; without a documented reference count there is nothing to validate against [S1][S2].	Reference-count procedure, counter briefing sheet, raw manual count records, and the matching rules used to align manual and automatic events.	
A3	The reference sample shall be designed to be representative across day types, times of day, operating states, demand patterns, vehicle types, door types and sensor types, and shall explicitly include unusual bulk boarding events.	A sample taken on quiet midweek daytime runs will pass almost any sensor. Peak crush loads, school journeys, buggies and wheelchairs are where counting fails [S2].	Sample design document showing the strata, the number of stop-door events per stratum, and how bulk-boarding journeys were selected rather than avoided.	
A4	The supplier shall submit the sample-size calculation, the raw matching rules and the confidence-interval or equivalence-test output, and not merely a headline accuracy figure.	The published VDV method is statistical: the result depends on sample size, error spread and the pre-set tolerance band, so the calculation is the claim [S2].	Sample-size calculation with stated assumptions, raw paired dataset, statistical output file, and the name of the person or body that produced it.	
A5	Where VDV-Schrift 457 is offered as the accuracy framework, the supplier shall name the version worked to, state that VDV identifies version 2.3 (11/2025) as current, and supply the prescribed evidence for the offered product scope. A vendor-wide "VDV certified" claim shall not be accepted.	VDV-Schrift 457 is an industry recommendation and framework issued by the Verband Deutscher Verkehrsunternehmen, not a UK statutory or ISO certificate, and the issuer page does not confer a vendor-wide certificate [S1].	Statement of the version used; the vehicle, door, sensor and firmware scope; the validator's identity and independence; the acceptance dataset; and the re-test regime.	
A6	Where published VDV numerical limits are used as the acceptance basis, the tender shall state that they are taken from the publicly available English Recommendation 457 v2.1 (04/2018): compensatory total error not exceeding 5%; global difference between summed automatic and manual boardings and alightings not exceeding 1% at the verification level; and not more than 5% of door-stop events faulty (deviation above 33.3% and more than one passenger against the manual count), or alternatively not more than 5% of vehicle halts faulty (above 20% and more than one passenger).	These are the only VDV 457 figures that could be verified from a publicly accessible issuer text, so they are a transparent starting point rather than a claim about the current edition [S2].	Bidder's measured values against each of these limits, with the paired dataset, plus written confirmation of which edition the bidder actually tested to.	
A7	The tender shall record that the numerical tolerance tables of VDV 457 v2.3 (11/2025) were not publicly verifiable at the date of this checklist, and shall require the successful bidder to confirm the applicable limits from the current licensed VDV text before acceptance testing begins.	Buying to an out-of-date table, or to a table the bidder has quietly reinterpreted, is a dispute waiting to happen at acceptance [S1][S2][S14].	Written confirmation of the v2.3 limits from the licensed text, or a signed statement that the parties have agreed to use the v2.1 published limits as the contractual basis.	

Ref	Requirement	Why it matters	Evidence to request	Score
A8	Acceptance shall use an equivalence test: the whole 95% confidence interval for the mean relative error must lie inside a pre-set tolerance band $[-\Delta, +\Delta]$. Δ shall be stated in the contract.	An equivalence test prevents a wide, uncertain result from passing merely because its central estimate looks good [S2].	Equivalence-test output showing the confidence interval and the band, with the underlying paired data and the statistical software or script used.	
A9	Δ shall be set within the 1–2% span published by VDV by mode, with 1% used where the data informs revenue sharing; an authority's tender value shall not exceed 2%.	The published guidance recommends 1% for revenue sharing and advises that authority tender values should not exceed 2%, which gives buyers a defensible number instead of an argument [S2].	Contractual statement of Δ with the reason for the value chosen, and the bidder's evidence that it can meet that Δ on comparable vehicles.	
A10	A manual reference journey shall be eligible only where its own boarding and alighting reconciliation is within 2%, and the included journeys shall collectively reconcile within 1%; ineligible journeys shall be repeated or excluded under a rule stated before data collection.	Without an eligibility rule fixed in advance, a bidder can retrospectively discard the journeys that went badly [S2].	Per-journey reconciliation table showing eligibility, plus the pre-agreed rule for repeats and exclusions.	
A11	Boarding and alighting reconciliation shall be reported per door, per vehicle and per route, not only as a fleet total.	A fleet total hides a single failing door or a badly mounted sensor on one vehicle type, which is exactly the fault a validation is meant to find [S2].	Per-door, per-vehicle and per-route reconciliation report from the offered platform, generated by the buyer's own user account during acceptance.	
A12	The treatment of bulk boarding, standing loads, pushchairs, wheelchairs, luggage, staff movements and non-passenger door openings shall be documented, and its effect on the reported figures quantified.	These are the recurring causes of systematic under- or over-count, and buyers usually discover them after go-live rather than during evaluation [S2].	Written handling description per case plus measured results from a journey set that deliberately includes them.	
A13	Re-validation shall be triggered by any firmware change, sensor replacement, mounting change, door reconfiguration or vehicle-type extension affecting the count core, in addition to a periodic re-test at a stated interval.	VDV distinguishes initial, event-related and periodic recertification, and v2.3 specifically refers to change-impact evidence for firmware changes; accuracy proven once is not accuracy proven forever [S1] [S2].	Change-control policy showing which change classes trigger re-validation, plus the re-test report from the most recent firmware release on a comparable deployment.	
A15	Bidders may offer a non-UK methodology comparator. Where the US Federal Transit Administration National Transit Database approach is cited, the buyer shall note that it requires an approved APC benchmarking and maintenance plan and that annual random-sample estimates must meet 10% precision at 95% confidence — a methodology reference only, and not evidence of UK compliance.	It is a genuinely independent prescribed process and useful as a cross-check on a bidder's statistical literacy, but it answers a US reporting duty, not a UK one [S3].	The bidder's benchmarking and maintenance plan, or a statement that this comparator is not being relied upon.	

Section B — Sensors and vehicle fit

No UK primary source establishes a universal PSV camera or APC mounting standard, so the contract must be vehicle-specific with OEM or bodybuilder sign-off [S9][S12]. Environmental and EMC qualification should be cited from road-vehicle standards, not rail.

Ref	Requirement	Why it matters	Evidence to request	Score
B1	The supplier shall provide a mounting design per vehicle type in the fleet, stating saloon height range, sensor height, offset from the door aperture, field of view and the resulting counted zone.	Overhead counting sensors are geometry-dependent: a design proven on a single-deck low-floor vehicle may not hold on a double-deck stairwell or a coach-height saloon.	Per-vehicle-type mounting drawings with dimensions, a photographic survey of at least one vehicle per type, and the sensor's declared minimum and maximum mounting height.	
B2	Door coverage shall be stated explicitly: which doors are counted, how many sensors per door, and how the design handles wide, double-leaf or rear doors and doors used for both boarding and alighting.	Partial door coverage is the most common hidden gap in an APC deployment and it invalidates route-level reconciliation.	Door-by-door coverage matrix per vehicle type, and the stated behaviour when a door is used contrary to the normal boarding pattern.	
B3	Power draw per sensor and per vehicle installation shall be stated, with behaviour on ignition-off, low-voltage and battery-protection conditions.	Sensing kit that flattens a battery overnight, or that silently stops recording when the vehicle enters battery protection, produces missing data that looks like low patronage.	Measured current draw at nominal and worst case, the ignition and shutdown logic, and any vehicle electrical approval required.	
B4	Each supplied enclosure shall have a declared ingress-protection rating classified and tested under the IEC 60529 IP Code, appropriate to its actual mounting location (interior protected, doorway, roof or external), including the connector and cable-gland boundary.	IEC 60529 classifies protection but does not choose a level for a bus; an unqualified "IP-rated" claim tells the buyer nothing about the doorway environment [S8].	Declared IP rating per part number with test evidence, plus a statement of the connector and gland boundary conditions assumed.	
B5	Environmental and mechanical qualification shall be evidenced against the ISO 16750:2023 series for road vehicles — Part 1 general, Part 2 electrical loads, Part 3 mechanical loads including vibration, Part 4 climatic loads, Part 5 chemical loads — with the declared mounting class matching the real mounting location.	ISO 16750 selects tests by mounting location, so a bare "ISO 16750 compliant" assertion without the test plan and declared class is not evidence [S6].	Test plan and test report per applicable part, with the declared mounting class, sample identity and test-house identity.	
B6	BS EN 50155 shall not be accepted as bus vehicle-fit evidence. It may be offered only as additional environmental evidence where the buyer expressly chooses to consider it.	EN 50155 is a railway rolling-stock electronic-equipment standard; citing it for a PSV substitutes an impressive-sounding number for the relevant road-vehicle qualification [S7].	If offered, a written explanation of which clauses the buyer is being asked to accept and why, alongside the ISO 16750 and UN R10 evidence.	
B7	Electromagnetic compatibility shall be evidenced under UN Regulation No. 10, Revision 6 (06 series) for the supplied electronic unit, its configuration and its installation, with confirmation that retrofit wiring and antennae do not defeat the vehicle's existing type approval.	UN R10 covers EMC approval for vehicle categories including M (buses) and for components and separate technical units intended for fitment; a self-declared "E-mark compatible" badge is not type-approval evidence [S5].	Approval or E-mark documentation with approval number and scope, the installation configuration tested, and a signed statement on the effect of retrofit wiring and antennae.	

Ref	Requirement	Why it matters	Evidence to request	Score
B8	The installation shall not obstruct or reduce compliance with the Public Service Vehicles Accessibility Regulations 2000 (SI 2000/1970). The supplier shall carry out an installation survey and provide signed assurance that sensors, cameras, displays, brackets, cabling and maintenance access do not obstruct wheelchair or priority space, gangways, handrails, signage, boarding equipment or passenger safety features.	PSVAR regulates vehicle accessibility; it does not approve a camera position, so the assurance has to come from the installer and the vehicle engineering function [S9].	Installation survey report per vehicle type and signed accessibility assurance naming the responsible engineer.	
B9	Where the design changes passenger space or information provision, the buyer shall apply accessibility principles and user testing. "DPTAC approved" shall not be accepted as a status.	The Disabled Persons Transport Advisory Committee is an independent expert committee that advises government; it is not a certifier of products or mounting positions [S10].	Accessibility impact note and, where relevant, user-testing record. Reject any claim of DPTAC approval absent a specific formal approval document.	
B10	The contract shall be vehicle-specific: OEM or bodybuilder approval where required, structural, fire, electrical and sight-line assessment, no safety or accessibility obstruction, documented wiring protection, post-installation inspection, and explicit responsibility for restoring compliance if an installation is found non-compliant.	No UK primary source establishes a universal PSV camera or APC mounting standard, so vehicle-specific sign-off is the only defensible route [S12].	OEM or bodybuilder written approval where required, assessment records, post-installation inspection sheets, and a named remediation liability in the contract.	

Section C – Gateway, connectivity and resilience

The vehicle is a hostile network environment. This section tests whether the data survives the journey.

Ref	Requirement	Why it matters	Evidence to request	Score
C1	The on-vehicle gateway shall be a purpose-built cellular device with stated model, cellular bands, antenna arrangement and mounting, and shall not depend on a PC, tablet, logged-in user session or manually started application.	Any solution that needs someone to log in or leave a laptop running will lose data on the first driver change.	Gateway specification, photographs of the installed device, and a written statement of the boot and unattended operation behaviour.	
C2	All data leaving the vehicle shall be encrypted in transit using TLS, with the protocol version, cipher policy and certificate validation behaviour stated.	Unencrypted telemetry over a public mobile network is an avoidable exposure and is difficult to defend in a DPIA.	Protocol and TLS version, certificate and trust-store configuration, and evidence that server certificate validation is enforced rather than disabled for convenience.	
C3	The gateway shall store and forward through signal gaps, tunnels, depots and out-of-coverage running, with a stated local buffer capacity in records and in hours of service.	Coverage gaps are routine on UK bus routes; without buffering, missing data is indistinguishable from an empty bus.	Buffer size in records and hours, the flush behaviour on reconnection, and a demonstration or log extract from an induced outage.	
C4	Buffered records shall retain the original source timestamp from the point of measurement; the platform shall not substitute the time of receipt.	If a late-arriving batch is stamped with the receipt time, an hour of boardings lands in the wrong hour and per-hour reporting becomes worthless.	Record schema showing source and receipt timestamps as separate fields, plus a worked example of a delayed batch landing in the correct period.	
C5	The behaviour on gateway restart, power cycle and firmware update shall be stated, including whether buffered records survive and whether the sensing chain resumes without human intervention.	A device that loses its buffer on reboot will lose data at exactly the moments it is most likely to reboot.	Documented restart behaviour and a log extract showing recovery and buffer persistence across a power cycle.	

Ref	Requirement	Why it matters	Evidence to request	Score
C6	SIM provision, data-plan ownership, roaming policy, data volume per vehicle per month and the consequences of exceeding an allowance shall be stated, together with who owns the SIM at contract end.	Supplier-owned SIMs on a supplier-owned plan are a quiet lock-in and can throttle data silently at month end.	Data volume estimate per vehicle, plan ownership statement, and the contractual position on SIM transfer or replacement at exit.	
C7	Remote configuration and firmware update shall be controlled: only authorised named individuals shall be able to push changes, changes shall be logged, and the buyer shall be notified before any change affecting the count core.	An unannounced firmware push can invalidate the accuracy validation without anyone noticing until the numbers move [S1].	Change-control procedure, access list, sample change log, and the notification commitment in the contract.	
C10	Time synchronisation on the vehicle shall be specified, including the source, the maximum tolerated drift and the behaviour when synchronisation is lost.	Per-hour and per-stop reporting depends on clocks; unsynchronised vehicle clocks shift counts between periods.	Time source specification, drift tolerance, and the flag or exception raised when a vehicle clock is out of tolerance.	

Section D — Data platform and storage

Where the data rests, whether it survives, and whether its provenance can be traced.

Ref	Requirement	Why it matters	Evidence to request	Score
D1	The supplier shall state where data is stored, in which country or region, on what class of storage, and under whose account or subscription.	The buyer cannot answer a DPIA question about hosting or a continuity question about ownership without this [S17] [S18].	Hosting and region statement, storage architecture diagram, and the name of the account holder for each environment.	
D2	Stored records shall persist across service restarts, container replacements and platform redeployments, and the persistence mechanism shall be described.	Analytics platforms deployed on ephemeral hosting can silently lose history at the next redeploy, and the loss is often noticed only at year end.	Persistence design (for example a named persistent volume or managed database), plus evidence of history surviving a deliberate redeploy during acceptance.	
D3	Long-period analytics shall be produced by aggregating stored per-day records, and shall not be derived by reading live cumulative sensor totals.	Cumulative sensor counters reset, roll over and drift; aggregating stored daily records keeps annual figures reconstructable and auditable.	Written description of the aggregation path from raw record to yearly figure, plus a reconciliation of one month of daily records against the reported monthly and yearly totals.	
D5	Location data shall carry provenance fields that distinguish measured positions, cached or stale last-known positions, scheduled or interpolated positions, and bench-test coordinates.	Without provenance, a failed antenna can pin a vehicle to one location and the map still looks plausible.	Record schema with the provenance fields, the permitted values, and a sample export showing each value in use.	
D6	Stale positions shall expire rather than being presented as current, with the expiry threshold stated and configurable.	A last-known position shown as live is worse than no position, because it is trusted.	Stated expiry threshold, the display or API behaviour after expiry, and a demonstration on a vehicle with a disconnected position source.	
D8	Backup and restore shall be specified: frequency, retention, encryption, storage location, and a tested recovery-time and recovery-point objective.	An untested backup is a plan, not a control.	Backup policy, most recent restore-test record with date and outcome, and the stated RPO and RTO.	
D9	An audit trail shall record data corrections, deletions, configuration changes, schema or version changes and administrative actions, with actor and timestamp, and shall be exportable to the buyer.	Funding claims and revenue-sharing disputes are settled by audit trails, not by dashboards [S2].	Audit-log schema, a sample export, the retention period, and confirmation that the buyer can obtain it without asking the supplier to extract it manually.	

Ref	Requirement	Why it matters	Evidence to request	Score
D10	Data ownership shall be stated unambiguously in the contract: the buyer owns its counting and location data, with any supplier rights to aggregated or anonymised use set out explicitly and capable of being refused.	Ambiguous ownership clauses are where benchmarking products quietly get built out of an operator's data.	Draft data-ownership and licence clauses, plus a written statement of every secondary use the supplier intends.	
D11	The record schema shall be published, with field names, types, units, nullability and the meaning of every status or flag value.	A published schema is the difference between an integration project and an archaeology project.	Schema document or machine-readable definition covering every field the buyer can retrieve via export or API.	

Section E — Data quality and observability

A silent failure that nobody sees is worse than a loud one. These rows put liveness and coverage into the contract rather than leaving them to the supplier's discretion.

Ref	Requirement	Why it matters	Evidence to request	Score
E1	Feed liveness thresholds shall be stated in the contract as numbers, not described as "monitored". As a worked example, a deployment may define 45 minutes without data as stale and 120 minutes as offline.	Without contractual thresholds, "we monitor the feed" is unenforceable and every outage becomes a conversation about whether it counted.	Stated thresholds, the alert routing, and evidence of a real alert firing during a genuine gap in service.	
E2	Alerting shall be demonstrated on the live feed rather than described, including the elapsed time between the last record and the alert.	Monitoring that only reports process health will happily report "healthy" while no data arrives.	Alert record from a real gap, with timestamps for last data, alert raised and alert received.	
E3	The known fleet shall be seeded so that the coverage denominator is fixed: a vehicle that stops reporting shall appear as missing, not disappear from the fleet list.	If the denominator is "vehicles that reported today", a broken vehicle improves the apparent coverage figure.	Fleet-register mechanism, and a coverage report showing a non-reporting vehicle still present and flagged.	
E4	Expected shutdown windows shall be classified as expected states rather than faults, with the classification rule and the resulting record type stated.	Alert fatigue destroys monitoring: an operator that gets a fault alert every night will ignore the one that matters.	Classification rules for expected shutdowns, sample records, and the effect on availability reporting.	
E5	Derived analytics and alerts shall be suppressed, or clearly marked as unreliable, when the underlying source data is untrusted or a door feed is faulty.	A welfare, crowding or dwell inference built on a broken count is a confident wrong answer.	Gating logic linking derived outputs to sensor-health state, and evidence of suppression during a real sensor fault.	
E6	Data-loss rate shall be reported per vehicle and per period, distinguishing sensor loss, gateway loss, transport loss and ingest rejection.	A single loss percentage cannot be acted on; a categorised one points at the component to fix [S2].	Data-loss report for a recent month on a comparable deployment, with the categories and the calculation method.	
E7	A data-quality summary shall be available to the buyer for any reporting period, covering vehicle coverage, door coverage, loss rate, stale-position incidence and correction volume.	Buyers need to be able to state the quality of the data alongside the number when it is used in a funding case or a board paper.	Sample data-quality summary for one month, generated from the buyer's own account.	

Section F — Integration and open data

Interoperability standards are references, not certificates. Name the profile, the version and the mandatory test cases, and ask whether a claimed label is actually held [S15][S16].

Ref	Requirement	Why it matters	Evidence to request	Score
F1	The supplier shall provide programmatic access, over MQTT and REST, to the same records the dashboard reads, with no reporting figure available only inside the supplier's own user interface.	If the API returns a different figure from the dashboard, the buyer has two versions of the truth and no way to audit either.	API documentation, a live sandbox or test credentials during evaluation, and a reconciliation showing an API response matching the dashboard for the same period.	
F2	Per-stop and per-hour boardings and alightings shall be retrievable from a real endpoint computed from stored events, and shall not be a proportional estimate derived from route totals.	Estimated per-stop figures are frequently mistaken for measurements and then used to justify stop changes.	Endpoint specification, a sample response, and a written statement of whether the values are measured or modelled at each granularity.	
F3	Scheduled exports shall be available in CSV, Excel and PDF, with a documented file naming convention, schema stability commitment and a change-notice period for schema changes.	Downstream spreadsheets and warehouse loads break silently when a column is renamed without notice.	Sample exports of each type, the schema definition, and the contractual change-notice period.	
F4	A push route to the buyer's own environment shall be available — data-warehouse load or SFTP delivery — with stated frequency, format and failure handling.	Authorities increasingly need the data in their own analytics estate, not only in a supplier portal.	Push mechanism specification, a sample delivery, and the retry and alerting behaviour on failed delivery.	
F5	Where ITxPT is required, the tender shall name the specification and version — for passenger counting, S04P05 Passenger Counting v1.1.0 — together with the interfaces and mandatory test cases, and shall require the supplier to state whether it actually holds the ITxPT label.	The ITxPT label is the association's quality seal that a product complies with the applicable specifications; supporting an interface is not the same as holding the label [S4] [S15].	Specification and version worked to, interface list, test-case results, and the label certificate with scope and date if claimed.	
F7	Where planned or static data interchange is in scope, NeTex shall be named with the required UK profile and release, and shall not be cited as a real-time telemetry protocol.	NeTex is the CEN/TC 278 planned-data family based on Transmodel, appropriate for network, timetable and fare interchange — including BODS fares — not for APC telemetry [S16].	Statement of the NeTex profile and release supported, with a validated sample file.	
F8	Where real-time interfaces are in scope, the relevant SIRI service shall be named — SIRI-VM for monitored vehicle journey and location data, SIRI-SX for disruptions and situations — with the profile, UK extensions and field cardinality stated. "SIRI support" in general shall not be accepted.	SIRI is a family of services under EN 15531 Parts 1–3 and TS 15531 Parts 4–5; a generic claim does not say which service is implemented [S17].	Named services, profile document, field-level cardinality table, and a validated sample message per service.	
F9	Where consumer-facing crowding information is required, the supplier shall state whether it publishes GTFS Schedule and GTFS-Realtime, and specifically how VehiclePosition.occupancy_status is populated, its update latency, and how unknown or stale values are handled.	occupancy_status in the GTFS-Realtime Reference v2.0 is an optional interoperability field, not evidence that a count is validated [S18][S19].	Field-mapping document from internal counts to occupancy_status, latency figures, stale-handling rule, and a sample feed.	
F10	The supplier shall state clearly whether a published occupancy value is APC-derived or estimated, at the field level.	An estimated crowding value presented as a measurement misleads passengers and, eventually, the authority.	Field-level provenance statement and the display or API flag that carries it.	

Ref	Requirement	Why it matters	Evidence to request	Score
F11	For services in England, the tender shall set out the Bus Open Data regime context: the Bus Services Act 2017 provides the statutory basis, and the Public Service Vehicles (Open Data) (England) Regulations 2020 (SI 2020/749) require provision, through the designated bus open-data service, of timetable, vehicle-location, fares and ticket, and historic punctuality information for registered relevant local services, subject to the stated exclusions and the phased timetable.	These four categories are the statutory ones; conflating them with occupancy publication misstates the duty [S20][S21][S22].	The bidder's statement of which BODS categories it supports, in which format, and which remain the operator's responsibility.	
F12	The tender shall record that occupancy in the DfT BODS SIRI-VM profile is an optional field — alongside departure boarding activity and no-boarding-if-full — while core location fields are mandatory, and that occupancy is therefore not, on the sources checked, a standalone statutory BODS dataset duty. Occupancy publication shall be specified as a contract requirement with defined coverage and quality if the buyer wants it.	"BODS compliant" is a claim about somebody's publication duty, not about a sensor; buyers should specify the field, coverage and quality they want rather than assume the law does it for them [S22].	Written confirmation of which optional fields are populated, the coverage percentage of the fleet, and the quality rule applied before a value is published.	

Section G — Security

Ask for security evidence proportionate to the risk, and check the certificate scope and the legal entity name [S23][S24].

Ref	Requirement	Why it matters	Evidence to request	Score
G2	Dashboard and platform access shall use per-user authentication with individually named accounts. Shared passwords shall be prohibited as a contract requirement.	Shared dashboard passwords are common in this market and they defeat access logging, leaver management and any meaningful audit trail. Make removal a contractual requirement, not a hope.	Evidence of per-user accounts in the offered product version, the leaver process, and — where per-user authentication is a roadmap item — a dated commitment and an interim control.	
G3	Role-based administration shall be provided, with at least a read-only reporting role, an operational role and an administrator role, and least privilege applied by default.	Everyone holding an administrator account is the most common cause of accidental configuration damage.	Role matrix showing permissions per role and evidence that a read-only user cannot change configuration.	
G4	Login and administrative-action auditing shall be enabled, retained for a stated period and exportable to the buyer.	Without login auditing, the buyer cannot answer who saw or changed what, which is also a DPIA question [S17].	Audit-log sample, retention period, and the export route available to the buyer.	
G5	Broker and messaging permissions shall be least-privilege: per-device or per-service credentials restricted to the topics they need, with no shared wildcard publisher or subscriber.	One compromised vehicle credential with wildcard rights exposes the whole fleet's data.	Broker access-control configuration extract, and confirmation that a vehicle credential cannot read other vehicles' topics.	
G6	All credentials used during development, trial or pilot shall be rotated before go-live, removed from source code and configuration files, and held in a secrets store.	Pilot credentials pasted into a repository or a wiki page are among the most frequent real-world breach routes.	Rotation record with dates, secrets-management approach, and evidence that no credentials remain in code.	

Ref	Requirement	Why it matters	Evidence to request	Score
G7	Encryption in transit shall be enforced on every hop — vehicle to broker, broker to ingest, ingest to database, platform to browser and platform to integration — with encryption at rest stated where personal data is held.	A single unencrypted internal hop undermines the whole chain and is hard to explain to a DPO.	Hop-by-hop encryption statement with protocol and version, plus configuration evidence.	
G8	Development, test and production environments shall be isolated, with separate services, databases, storage and messaging identities, and no production personal data in test.	Shared environments allow development work to disrupt a live service or leak live data into a test system.	Environment diagram, separation evidence, and the policy on test data.	
G9	Releases shall be health-gated: a failed health check shall leave the previous working release serving, and rollback shall be documented and demonstrable.	The buyer's service should not depend on the supplier's deployment day going well.	Health-check endpoint and gating configuration, rollback procedure, and an example of a failed deployment that did not affect service.	
G10	A vulnerability management and patching process shall be evidenced, covering dependency and firmware vulnerabilities, severity-based remediation targets, and how the buyer is informed of a relevant issue.	On-vehicle devices and their dependencies age; a supplier with no patch cadence is accumulating risk on the buyer's fleet [S24].	Patch policy with remediation targets by severity, most recent scan or penetration-test summary, and a software bill of materials where available.	
G11	An incident-response and breach-notification process shall be provided, including the notification timescale to the buyer as controller.	The controller's own regulatory clock starts when it becomes aware, so a slow supplier notification is a compliance problem for the buyer [S17].	Incident-response plan, contact route, contractual notification timescale, and evidence of a test or a real incident handled.	
G12	Cyber Essentials or Cyber Essentials Plus may be required proportionately, in particular where the solution connects to operational technology, uses remote support or holds personal data. Certification shall be in the name of the legal supplier entity, current, and scoped to the offered service.	Cyber Essentials was developed by the NCSC as the government's minimum recommended cyber-security standard, and certification is assessed through the official scheme; a lapsed or out-of-scope certificate is not evidence [S23].	Current certificate with entity name, scope, certification body and expiry date.	
G13	ISO/IEC 27001 certification may be requested where proportionate, with the certificate scope in the supplying entity's name. Where the supplier is not certified, the buyer shall instead require a security questionnaire, architecture and data-flow documentation, penetration-test summary, vulnerability and patch process, key management, access logging, incident response, backup and continuity, and supply-chain controls.	ISO/IEC 27001 is common tender evidence of an information-security management system but is not a statutory prerequisite for an APC supplier; an uncertified internal policy is not a certification [S24].	Certificate with scope statement and accreditation body, or the full alternative evidence set above.	

Section H — Privacy and data protection

“GDPR compliant” and “anonymous” are deployment-specific legal conclusions reached by the controller, not product features a supplier can sell [S25][S30].

Ref	Requirement	Why it matters	Evidence to request	Score
H1	The supplier shall state whether the counting path is genuinely anonymous or pseudonymous, and shall justify the answer at the level of the data actually processed on the device and in the cloud.	An irreversibly aggregated count that cannot identify or single out a person falls outside UK GDPR, but pseudonymisation is not anonymisation [S28].	Data-flow description from sensor to store with the exact fields at each stage, plus a re-identification risk assessment.	

Ref	Requirement	Why it matters	Evidence to request	Score
H2	A camera-based counter shall not be described as anonymous merely because it does not retain a visible video clip. The supplier shall state what is processed in memory, what is written to storage and what is transmitted.	The processing, not the retention of a clip, determines the classification [S28][S27].	Written statement per device of in-memory processing, on-device storage, transmitted payload and any image or frame retention, however brief.	
H3	The supplier shall provide a complete data map: every field leaving the vehicle, its purpose, its recipients, its retention and its storage location.	The buyer as controller cannot complete a DPIA or a privacy notice without it [S26].	Field-level data map, list of processors and sub-processors, and hosting locations.	
H4	A retention schedule shall be stated per data category — raw events, aggregated counts, location records, diagnostic logs, audit logs and any imagery or analytics events — with automated deletion at the end of the period.	Retention that depends on somebody remembering to delete is not a control [S26].	Retention schedule with periods and deletion mechanism, plus evidence that deletion actually runs.	
H5	The supplier shall provide DPIA inputs to support the buyer's assessment under UK GDPR Article 35, and shall not assert that a DPIA is unnecessary.	Article 35 requires the controller to carry out a DPIA before processing likely to result in a high risk, particularly with new technologies; Article 35(3) expressly includes systematic monitoring of a publicly accessible area on a large scale [S25].	Supplier DPIA input pack: data-flow map, data categories, retention, processors and sub-processors, access controls, re-identification risk and residual-risk register.	
H6	The supplier shall assist with the DPIA process expected by the ICO: describing the processing and purposes, assessing necessity and proportionality, identifying risks to individuals and documenting the measures that address them, including support for consultation where appropriate.	The ICO treats a DPIA as good practice for any major personal-data project and expects documented screening even where the controller concludes one is not needed [S26].	Completed supplier sections of the buyer's DPIA template, and a named contact for consultation and prior consultation support.	
H7	The supplier shall confirm whether any component processes facial images or other data for the purpose of uniquely identifying a person, and shall flag any special-category processing.	"Biometric data" is defined in UK GDPR Article 4, and biometric data used to uniquely identify a person is special-category data under Article 9, requiring an Article 9 condition and a higher-risk assessment [S29][S30].	Per-component statement of whether unique identification occurs, the algorithmic function, and the Article 9 analysis where applicable.	
H8	The buyer shall record its lawful basis and the supplier shall support it: a public authority or LTA will often assess public task under Article 6(1)(e), requiring a task or function laid down in law and necessity; a commercial operator may assess legitimate interests under Article 6(1)(f), requiring a documented purpose, necessity and balancing assessment.	Neither basis is automatic, contractual necessity is not a shortcut for surveillance, and consent is rarely practical for routine onboard systems [S31][S32].	Lawful-basis assessment (buyer-owned) with the supplier's supporting technical description; legitimate-interests assessment where relied on.	
H9	Function creep shall be prohibited: no new analytic, no new retention, no new recipient and no remote viewing capability shall be enabled without the buyer's written approval and an updated DPIA.	Sensing platforms accumulate features; a counting deployment can drift into surveillance through configuration alone [S27].	Contractual change-control clause covering analytics and retention, plus the technical control that prevents silent enablement.	
H10	Where imagery, remote viewing or behavioural analytics are in scope, the buyer shall distinguish a privacy-preserving count from video retention, remote viewing and analytics, and shall set signage, transparency notices, subject-rights support, retention and secure export controls accordingly.	Identifiable video, linked vehicle or device identifiers, faces, behaviour and journey records can all be personal data, and the operator must apply the data-protection principles to them [S27].	Separate specification and evidence for the counting function and for any imagery or analytics function, plus draft signage and notice wording.	

Ref	Requirement	Why it matters	Evidence to request	Score
H11	Sub-processors and hosting locations shall be listed, with a change-notification and objection right for the buyer, and international transfer arrangements stated where relevant.	The controller remains accountable for the whole chain, including a sub-processor it has never heard of [S26].	Sub-processor list with purpose and location, the notification mechanism, and transfer safeguards where applicable.	
H13	"GDPR compliant" and "anonymous" shall not be accepted as product attributes. The buyer shall record that these are deployment-specific conclusions dependent on retention, remote access, linkage, analytics, re-identification possibility and the controller's purpose.	Retention, access and linkage can change the conclusion after go-live, so the claim has to be re-tested against the deployment as built [S25].	Bidder's rewritten claim wording naming the product, version, configuration and the assumptions on which the privacy position depends.	

Section I — Reporting and usability

Reports are the part of the system the buyer actually lives with. Specify the outputs, not the technology.

Ref	Requirement	Why it matters	Evidence to request	Score
I1	The report set shall include, as a minimum: daily, weekly, monthly and yearly boardings and alightings; route and vehicle filters; per-stop and per-hour breakdowns; and a period-comparison view.	These are the views that answer the questions operators and authorities actually ask, and their absence is usually discovered after award.	Live demonstration of each view on representative data, plus screenshots in the bid.	
I2	Every reported figure shall be exportable in CSV and Excel, and every report shall be exportable to PDF including any charts shown on screen.	Board packs and funding submissions need fixed artefacts, not links to a dashboard that will look different next month.	Sample exports of each type generated from the buyer's own account during evaluation.	
I3	Per-stop and per-hour granularity shall be available in exports as well as on screen, with the same values as the API.	Analysts work in spreadsheets and warehouses; screen-only granularity forces manual transcription.	Export sample at stop and hour granularity, reconciled against the API and the dashboard.	
I4	Data-quality context shall be displayed alongside the figures: coverage, missing vehicles, stale positions, excluded records and correction volume for the period shown.	A number without its quality context invites overconfident decisions and undermines the figure when it is challenged.	Screenshot or demonstration of quality context shown with a report, not buried in a separate admin page.	
I5	Funding-evidence and board-pack outputs shall be available: a period summary suitable for inclusion in a business case, stating method, coverage and quality alongside the counts.	Counting data is frequently used to support funding claims, and a bare total will not survive scrutiny.	Example summary output from a comparable deployment, with the method and quality statement included.	
I6	User roles shall map to real jobs — for example depot or operations, planning or analysis, finance or funding, and administration — with access limited accordingly.	Role design determines whether the platform is actually used or worked around.	Role matrix mapped to the buyer's job families, and evidence of role enforcement in the product.	
I9	Report definitions shall be documented: for each figure, the source records, the aggregation, the exclusions and the rounding.	Two similar-looking reports that differ by 3% will consume weeks unless the definitions are written down.	Report definition catalogue covering every figure the buyer will rely on.	

Section J – Commercial, delivery and support

Structure the commercial terms so the buyer can stop, extend or leave. Name the actual route to market rather than claiming general framework approval [S35][S36][S37][S38].

Ref	Requirement	Why it matters	Evidence to request	Score
J1	Pricing shall be broken down into hardware, installation, connectivity, platform subscription, support and professional services, per vehicle and per year, for the whole contract term including any extension.	Bundled pricing hides the cost of the years after year one, which is where APC contracts get expensive.	Full price schedule with unit rates, indexation mechanism and the total cost of ownership over the term.	
J2	Per-user licence costs shall be stated and capped, or user counts shall be unlimited. Any cost that rises with the number of people who look at the data shall be disclosed at bid stage.	Per-user pricing quietly restricts who in the organisation is allowed to see the data, which defeats the point of buying it.	Licence model statement, the cost of adding users, and any cap or unlimited-use commitment.	
J3	Delivery shall be staged: a pilot on a stated number of vehicles and routes, with a validation plan, before any fleet-wide commitment; the buyer shall have a documented right not to proceed.	A pilot gate converts bid claims into measured evidence on the buyer's own vehicles before the money is committed.	Stage plan with entry and exit criteria per stage, and the contractual right not to proceed after the pilot.	
J4	Acceptance criteria shall be tied directly to the validation plan in section A, including the agreed Δ , the reference-count method, the per-door and per-route reporting, and the data-quality thresholds in section E.	Acceptance that is not tied to the validation method becomes a negotiation about opinions [S2].	Draft acceptance-test specification referencing the section A and E requirements, with pass and fail consequences.	
J5	Handover documentation shall be specified as a deliverable: as-built installation records per vehicle, configuration, credentials held by the buyer, schema, API documentation, runbooks and validation reports.	Undocumented deployments cannot be maintained by anyone except the original supplier.	Documentation list as a contract deliverable, with acceptance of handover as a payment milestone.	
J6	Exit and data portability shall be contractual: full historical data in an open format within a stated period, schema documentation, deletion certification, and hardware ownership and removal terms.	Exit terms agreed at the start cost nothing; exit terms negotiated at the end cost a great deal.	Draft exit clause with the export format, timescale, deletion evidence and hardware position.	
J7	Support hours shall match the buyer's actual operating hours, including early mornings, late evenings, weekends and public holidays where services run.	Business-hours support on a service that runs from 05:00 to 00:30 leaves most of the operating week uncovered.	Support-hours schedule mapped to the buyer's service pattern, with the out-of-hours route and escalation path.	
J8	Response and fix targets shall be stated by severity, with the definitions of each severity, the measurement method and the remedy for failure.	"Best endeavours" is not a target, and an unmeasured target is not enforceable.	Severity definitions, response and fix targets, reporting method, and service-credit or remedy mechanism.	
J10	Insurance and company evidence shall be provided proportionately: employers', public and product liability, professional indemnity where relevant, accounts or turnover evidence, prior deployments and implementation capability, with exact policy limits and expiry dates.	These are risk-proportionate selection and contract requirements under the Procurement Act 2023 regime, not sector certifications, and "fully insured" is not an answer [S38].	Certificates of insurance with limits and expiry, financial statements, and named reference deployments with contactable referees.	
J11	The procurement route shall be stated in the tender documents: for new covered procurements the Procurement Act 2023 applies from 24 February 2025, with notices published through Find a Tender, which since that date carries above- and below-threshold notices other than below-threshold Scotland notices.	Bidders and buyers alike need to know whether this is an open tender under the Act or a call-off, because the rules and timescales differ [S35][S36][S37].	The notice reference, the procedure used, and the timetable.	

Ref	Requirement	Why it matters	Evidence to request	Score
J12	Where a framework or dynamic purchasing system route is used, the actual framework or DPS shall be named with its reference, lot, scope, expiry and the call-off authority's eligibility. Claims of general framework approval shall not be accepted.	A supplier being on some framework somewhere says nothing about whether this contract can be called off under it; scope and buyer eligibility must be checked [S39][S40].	Framework or DPS name and reference, lot, current status, scope confirmation covering APC and on-vehicle sensing, and the buyer's eligibility to use it.	
J14	Change control and price stability shall be contractual: notice periods for price changes, the mechanism for adding vehicles or routes, and the cost of extending scope.	Fleet changes are certain; the price of change should be known before award.	Change-control procedure and a rate card for additional vehicles, routes, users and integrations.	

Ten claims to challenge

Common vendor claims and the follow-up question that tests each one. Use these as clarification questions, and record the answer in your moderation notes.

#	The claim	What to ask, and why
1	"Our system is 99% accurate."	99% of what, measured how? Give the metric and denominator, the number of stop-door events in the sample, the day types and vehicle and door types covered, the firmware version, the confidence interval, the exclusion rules and the date. Then show the per-door and per-route breakdown. An unqualified percentage has no defined denominator, population, reference procedure or confidence interval [S13].
2	"We are VDV certified."	Which document, which version, and who certified what? VDV-Schrift 457 is an industry recommendation and framework issued by VDV, and the issuer identifies v2.3 (11/2025) as current; the issuer page does not confer a vendor-wide certificate. Ask for the tested scope (vehicle, door, sensor, firmware), the validator's identity and independence, the acceptance dataset and the re-test regime [S1][S14].
3	"We are ITxPT compliant."	Do you hold the ITxPT label, for which product and which specifications? The label is the association's quality seal that equipment, software or a service complies with the applicable specifications, which is not the same as supporting an interface. For counting, ask specifically about S04P05 Passenger Counting v1.1.0, the interfaces implemented and the mandatory test-case results [S4][S15].
4	"We are BODS compliant."	Compliant with which duty, and whose duty is it? The statutory categories under the Public Service Vehicles (Open Data) (England) Regulations 2020 are timetable, fares and tickets, real-time vehicle location and historic punctuality. Occupancy is an optional field in the BODS SIRI-VM profile, so ask which fields you populate, at what coverage, and what remains the operator's responsibility [S21][S22].
5	"The product is GDPR compliant."	Compliance is a conclusion about our processing, not a feature of your product. Give the field-level data map, retention per category, processors and sub-processors, hosting locations, access controls and re-identification risk, and tell us which of our controller obligations you are supporting and which remain ours [S25][S26].
6	"It is an anonymous AI camera."	What is processed in memory, what is written to storage and what is transmitted? An irreversibly aggregated count that cannot single out a person is outside UK GDPR, but pseudonymisation is not anonymisation, and not retaining a visible clip does not make the processing anonymous. If any component processes facial images for unique identification, Article 4 and Article 9 are engaged [S28][S29][S30].
7	"You will not need a DPIA."	That is our decision as controller, and we will document it either way. Article 35 requires a DPIA before processing likely to result in high risk, and Article 35(3) expressly includes systematic large-scale monitoring of publicly accessible areas. Supply DPIA inputs rather than a conclusion; the ICO expects documented screening even where we decide a DPIA is not required [S25][S26].
8	"We are ISO 27001 certified."	Show the certificate: which legal entity, which accreditation body, what scope statement, and what expiry date? ISO/IEC 27001 evidences an information-security management system, but it is not a statutory prerequisite here, and an internal policy modelled on the standard is not certification. If the scope excludes the offered service, we will ask for the alternative evidence set instead [S24].

#	The claim	What to ask, and why
9	"We provide real-time occupancy."	How real-time, from what, and how do you handle staleness? State the end-to-end latency from door event to published value, the buffering behaviour through coverage gaps, whether the value is APC-derived or estimated, and how unknown or stale values are represented. In GTFS-Realtime, occupancy_status is an optional field, not a validation [S19].
10	"We have an open API."	Open to whom, returning what? Give us documentation, test credentials during evaluation, and a reconciliation showing the API returning the same figures as the dashboard for the same period, at per-stop and per-hour granularity. Confirm that we hold our own credentials, that rate limits are documented, and that no reported figure exists only inside your interface.

Scoring summary sheet

Transfer the section means here. Weights are a starting point — adjust them to the risk you are carrying, and record the reason for any change in your evaluation strategy.

Ref	Section	Weight	Rows	Score (mean 0–3)	Notes and evidence gaps
A	Accuracy and validation	25%	14		
B	Sensors and vehicle fit	8%	10		
C	Gateway, connectivity and resilience	7%	8		
D	Data platform and storage	10%	9		
E	Data quality and observability	10%	7		
F	Integration and open data	10%	11		
G	Security	10%	12		
H	Privacy and data protection	10%	12		
I	Reporting and usability	5%	7		
J	Commercial, delivery and support	5%	12		
	Weighted total	100%	102		

Gates applied

- Any row scored 0 in sections A, G or H — clarification round before scoring is finalised.
- Mean score below 2 in section A — fail, regardless of the weighted total.
- No written validation plan (section A) or no signed vehicle-fit assurance (section B) — no award.
- Fleet rollout conditional on pilot evidence, not on the bid document (row J3).

Moderation record

Record, for each section: the evidence actually received, the rows where the bidder scored 1 rather than 2 or 3, the clarification questions asked, and the answers. This record is what makes the award defensible if it is challenged, and it is also the basis for the acceptance testing in row J4.

Sources

Every standard, regulation and guidance document cited in this checklist, with its issuing body and full URL. Bracketed references in the requirement tables point to this list.

Ref	Issuing body	Document and URL
S1	VDV (Verband Deutscher Verkehrsunternehmen)	VDV-Schrift 457 — Automatische Fahrgastzählsysteme (AFZS): current version page; issuer identifies v2.3 (11/2025) as current — https://www.vdv.de/afzs.aspx
S2	VDV (Verband Deutscher Verkehrsunternehmen)	VDV Recommendation 457 v2.1 (04/2018), publicly available English text — source of the published numerical limits quoted in section A — https://www.vdv.de/457-v2.1-ses.pdf
S3	US Federal Transit Administration (FTA)	APC data guidebook — NTD benchmarking and maintenance plan; 10% precision at 95% confidence (non-UK methodology comparator) — https://rosap.nhtl.bts.gov/view/dot/6456/dot_6456_DS1.pdf
S4	ITxPT	ITxPT Technical Specifications and the ITxPT label — https://www.itxpt.org/en/itxpt-specifications/
S5	UNECE WP.29	UN Regulation No. 10, Revision 6 — electromagnetic compatibility approval of vehicles and components — https://unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2019/E-ECE-324-Add.9-Rev.6.pdf
S6	ISO (ISO/TC 22/SC 32)	ISO 16750:2023 series — Road vehicles: environmental conditions and testing for electrical and electronic equipment (Parts 1–5) — https://www.iso.org/standard/77578.html
S7	BSI	BS EN 50155:2021 — Railway applications, rolling stock, electronic equipment (a rail standard, not bus vehicle-fit evidence) — https://knowledge.bsigroup.com/products/railway-applications-rolling-stock-electronic-equipment-1
S8	IEC (TC 70)	IEC 60529:1989+A1:1999+A2:2013 (edition 2.2) — Degrees of protection provided by enclosures (IP Code) — https://webstore.iec.ch/en/publication/2452
S9	UK legislation	The Public Service Vehicles Accessibility Regulations 2000 (SI 2000/1970) — https://www.legislation.gov.uk/uksi/2000/1970/contents
S10	GOV.UK	Disabled Persons Transport Advisory Committee (DPTAC) — advisory committee, not a certifier — https://www.gov.uk/government/organisations/disabled-persons-transport-advisory-committee
S11	ISO	ISO 16750-3:2023 — mechanical loads including vibration — https://www.iso.org/standard/77579.html
S12	UK legislation	PSVAR 2000 — referenced for the finding that no universal UK PSV camera or APC mounting standard was verifiable — https://www.legislation.gov.uk/uksi/2000/1970/contents
S13	VDV	VDV Recommendation 457 v2.1 — basis for the accuracy-claim risk position on unqualified percentages — https://www.vdv.de/457-v2.1-ses.pdf
S14	VDV	VDV 457 current page — basis for the finding that v2.3 numerical tolerance tables and any formal certificate scheme were not publicly verifiable — https://www.vdv.de/afzs.aspx
S15	ITxPT	ITxPT S04P05 Passenger Counting v1.1.0 announcement (succeeds and extends S02P07 Automatic Passenger Counting) — https://itxpt.org/upgrading-apc-considering-rail-requirements/
S16	CEN/TC 278 — NeTEx/Transmodel	NeTEx (Network and Timetable Exchange) implementation overview — https://netex-cen.eu/
S17	CEN/TC 278 — Transmodel	Standards for implementation overview — SIRI family including SIRI-VM and SIRI-SX (EN 15531 Parts 1–3, TS 15531 Parts 4–5) — https://transmodel-cen.eu/index.php/standards-for-implementation/
S18	MobilityData / GTFS community	GTFS Schedule Reference — https://gtfs.org/documentation/schedule/reference/

Ref	Issuing body	Document and URL
S19	MobilityData / GTFS community	GTFS-Realtime Reference v2.0 — VehiclePosition.occupancy_status — https://gtfs.org/documentation/realtime/reference/
S20	UK legislation	Bus Services Act 2017 — https://www.legislation.gov.uk/ukpga/2017/21/contents
S21	UK legislation	The Public Service Vehicles (Open Data) (England) Regulations 2020 (SI 2020/749) — https://www.legislation.gov.uk/uksi/2020/749/contents
S22	Department for Transport	Bus Open Data Service — operator requirements guidance, including the SIRI-VM profile in which Occupancy is optional — https://publish.bus-data.dft.gov.uk/guidance/operator-requirements/?section=buslocation
S23	NCSC	Cyber Essentials overview — https://www.ncsc.gov.uk/cyberessentials/overview
S24	ISO	ISO/IEC 27001 information security overview — https://www.iso.org/isoiec-27001-information-security.html
S25	UK legislation	UK GDPR Article 35 — Data protection impact assessment — https://www.legislation.gov.uk/eur/2016/679/article/35
S26	ICO	Data protection impact assessments — when a DPIA is needed and how to do one — 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/
S27	ICO	CCTV and video surveillance guidance — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/
S28	ICO	Anonymisation guidance — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/
S29	UK legislation	UK GDPR Article 4 — definitions, including biometric data — https://www.legislation.gov.uk/eur/2016/679/article/4
S30	UK legislation	UK GDPR Article 9 — processing of special categories of personal data — https://www.legislation.gov.uk/eur/2016/679/article/9
S31	ICO	Lawful basis — public task — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/public-task/
S32	ICO	Lawful basis — legitimate interests — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/
S33	UK legislation	Data (Use and Access) Act 2025 — https://www.legislation.gov.uk/ukpga/2025/18/contents
S34	ICO	DPIA guidance status page — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
S35	UK legislation	Procurement Act 2023 (c.54) — https://www.legislation.gov.uk/ukpga/2023/54/contents
S36	GOV.UK	Procurement Act 2023 — a short guide for suppliers — https://www.gov.uk/government/publications/procurement-act-2023-short-guides/the-procurement-act-2023-a-short-guide-for-suppliers-html
S37	Find a Tender service	Find a Tender — UK central digital service for procurement notices — https://www.find-tender.service.gov.uk/
S38	UK legislation	Procurement Act 2023, section 22 — conditions of participation — https://www.legislation.gov.uk/ukpga/2023/54/section/22
S39	Government Commercial Agency (formerly Crown Commercial Service)	Spark: Technology Innovation Marketplace, DPS RM6094 — https://www.crowncommercial.gov.uk/agreements/RM6094

Ref	Issuing body	Document and URL
S40	ESPO	ESPO framework solutions — https://www.espo.org/our-framework-solutions
S41	GOV.UK	PPN 06/20 — Social Value Model: taking account of social value in the award of central government contracts — https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts
S42	Home Office / UK legislation	Update to the Surveillance Camera Code of Practice (in force 12 January 2022) and Protection of Freedoms Act 2012, Part 2 Chapter 1 — https://www.gov.uk/government/publications/update-to-surveillance-camera-code

Research position 13 September 2026. “Current” means the latest version or status verifiable from the linked issuer, regulator or official standards catalogue on that date. Obtain the licensed text of any paywalled standard and confirm vehicle-specific approval applicability with the vehicle manufacturer or type-approval holder. Items deliberately recorded as unverified: the numerical tolerance tables of VDV 457 v2.3 and any formal VDV third-party certificate scheme; a universal UK PSV camera or APC mounting standard; and a standalone ISO or EN APC accuracy-certification standard.

How Smart Urban Sensing can help

We wrote this checklist to be used against us as well as against anyone else. If it is useful, these are the two things buyers most often ask us to do next.

Specification review before you go to market

We will read your draft ITT specification against this checklist and tell you where a bidder could answer yes without evidence: unbounded accuracy wording, missing reference-count method, absent liveness thresholds, open-data requirements that name a standard but not a profile, and privacy requirements that ask for a conclusion rather than an input. Output is a marked-up specification and a scoring sheet your evaluation panel can use.

Pilot with a written validation plan

We install on a stated number of vehicles and routes, agree the reference-count method, the sample design across day types and door types, and the tolerance band (delta) before the pilot starts, and report the result per door, vehicle and per route. If the pilot does not meet the agreed band, the report says so.

Integration and data-quality work

MQTT and REST access to the same records the dashboard reads, per-stop and per-hour boardings and alightings from a real endpoint, location provenance fields, contractual liveness thresholds and a data-quality summary alongside the counts.

Privacy and DPIA support

Field-level data maps, retention schedules and supplier DPIA inputs for your Article 35 assessment. We supply the inputs; the assessment and the lawful-basis decision remain yours as controller.

Where we draw the line

Scored against this document, this is what we stand behind and where we set the boundary, at the date of publication.

Smart Urban Sensing — our own position, scored against this checklist

We publish these so that a buyer can score us on the same terms as any other bidder:

- We publish no blanket accuracy percentage. Accuracy is validated per installation against manual reference counts, and the result is recorded per door and per route.
- The dwell signal in our welfare module is currently a proxy based on a 20-minute no-alighting window, not per-passenger dwell time. Native sensor dwell fields require validation before we make direct dwell claims.
- Welfare signals are commissioned per fleet: detection, classification, deduplication and storage are built and in place, and thresholds plus the acceptance test are set on the buyer's own vehicles before the signals go live to a control room. The camera holds no vehicle-specific certification for this application.
- Per-user authentication with role-based administration and login auditing is a roadmap item; dashboard access today uses a shared credential, so credential hardening and rotation are pre-deployment work (row G2).
- Open-data conformance we have not implemented is described as a roadmap item, including BODS and GTFS-Realtime occupancy export.
- We claim no certification without an audit: no VDV 457 certificate, no ITxPT label, no ISO/IEC 27001 certification, no Cyber Essentials claim, and no type-approval or accessibility approval beyond the evidence we can produce for a specific installation.
- Our reference deployment is a US healthcare-campus shuttle operation in daily scheduled service. We describe it anonymously — operator, fleet size and route detail stay confidential — and we do not extrapolate its results to a UK fleet without a local validation.

TALK TO US BEFORE YOUR ITT GOES OUT

Smart Urban Sensing Limited

Colony, 5 Piccadilly Place, Manchester M1 3BR

sales@smarturbansensing.co.uk

Specification review · validated deployment with a written validation plan · integration and data-quality work · supplier DPIA inputs

Reference deployment: a US healthcare-campus shuttle operation in daily scheduled service.