

PINPOINTERS PLATFORM DATA PROCESSING ADDENDUM (DPA)

Applies to: The telematics tracking data, standalone GPS coordinates, live video clips, still image thumbnails, and local driver alerts processed by Pinpointers on behalf of the commercial client (the Data Controller).

1. Scope and Object of Processing

This Addendum governs the processing of vehicle telematics, localization mapping, and video event records generated by hardware units supplied by Pinpointers. The client acknowledges that they dictate the purpose and parameters of tracking, making them the exclusive Data Controller under current UK and EU privacy laws.

2. Special Provisions for Vehicle Rental, Leasing, and Hire Clients

Where the Client utilizes Pinpointers hardware within vehicles destined for short-term rental, long-term commercial lease, or contract hire to downstream end-renters, the Client expressly acknowledges and agrees to the following statutory terms:

- **2.1 Mandatory In-Cabin Transparency Labeling:** The Client assumes sole legal responsibility to ensure that every vehicle fitted with an all-in-one Pinpointers device features clear, prominent, and highly visible text signage inside the cabin (e.g., dashboard or windscreen labeling). This signage must explicitly inform drivers that real-time GPS tracking, Edge-AI driving distraction analytics, and event-based video recording are operational.
- **2.2 Flow-Down Privacy Terms:** The Client must legally embed into their rental/hire agreements a clear privacy notice informing the end-renter that they will receive access to a telematics portal, and that they (the renter) assume the responsibilities of a Data Controller for their chosen operators.
- **2.3 Absolute Privacy Indemnity:** Pinpointers acts purely as a technology pipeline provider. The Client shall fully indemnify, defend, and hold harmless SBS Solutions Limited against any and all civil regulatory fines, litigation costs, or employee driver grievances resulting from the Client's or end-renter's failure to provide adequate transparency labeling or securing appropriate data authorizations.
- **2.4 Emergency Asset Protection and Theft Recovery Intercept:** Where the Client (the Rental/Leasing Company) requests administrative override permissions to access real-time or historical GPS location data—independent of the downstream renter's active portal account—for the exclusive purpose of vehicle theft recovery, asset preservation, or emergency asset localization, the Client expressly covenants and agrees that:
 - (a) The Client acts as an independent Data Controller for the duration of that specific emergency tracking event, relying on the lawful basis of 'Legitimate Interests' (asset protection) or 'Recognised Legitimate Interests' (crime prevention) under the Data (Use and Access) Act 2025.
 - (b) The Client holds sole legal responsibility for ensuring that its rental/hire agreements explicitly inform downstream renters that location tracking may be accessed by the vehicle owner strictly in the event of suspected theft, contract

- breach, or emergency.
- (c) Pinpointers provides this administrative access utility strictly as a technical sub-processor. Pinpointers will maintain automated platform audit logs of all emergency location requests, and the Client shall fully indemnify Pinpointers against any privacy claims or driver grievances arising from unauthorized or unlawful tracking overrides executed by the Client's administrative users. **The Client acknowledges that this emergency override feature is strictly limited to geographic telemetry data; administrative access to edge-processed cabin video or audio files during emergency intercept configurations is entirely hard-coded and locked out.**

3. Product Segmentations & Data Categories Processed

Depending on the specific hardware deployed across the client's fleet, the platform securely streams and logs:

- **Standalone GPS Tracking Hardware:** Real-time and historic GPS coordinate logs, vector speeds, time stamps, and custom placemarkers.
- **All-in-One Camera & Tracking Units:** Integrated, unified hardware assets capturing simultaneous geographic position telemetry alongside short, event-triggered video clip uploads.

4. Edge-AI Processing and Biometric Defensibility

For all-in-one models equipped with advanced driver analytics, systems execute driver fatigue, gaze tracking, and distraction analytics **entirely locally on the physical camera device (Edge-AI Processing)**.

- **Zero Biometric Transmission:** No biometric reference templates, unique facial mapping keys, or persistent raw interior camera streams are transmitted to, or archived on, our AWS cloud infrastructure.
- **Event Flares Only:** The hardware merely pushes an alphanumeric "Event Flag" to the platform to notify fleet managers of a distraction warning, allowing the manager to download the video clip of that specific event.

5. Audio Capture Default Deactivation Safe Harbor

- **Audio Disabled by Default:** Microphones contained within all dashcam devices are physically deactivated by default at the factory level.
- **Controller Authorization Obligation:** In-cabin audio recording will only be toggled on remotely by Pinpointers upon explicit, written authorization from the corporate Client. The Client assumes full legal responsibility to secure all required legal permissions, employee union approvals, or workforce handbook updates before requesting audio activation.

6. Multi-Region Infrastructure and Data Isolation

- **Centralized UK/EEA Footprint:** Platform services, file storage pools, and telematics routing databases run inside a combined infrastructure across **AWS London (UK) and AWS Ireland (EEA)** data center regions.
- **Access Segregation:** Customer user spaces are entirely sandboxed. Pinpointers

employs role-based permission architecture ensuring complete data separation across corporate environments.

7. Commercial Tiered Retention Lifecycles

The platform applies an automated data-purging architecture based on the Client's specific commercial contract subscription tier:

- **Standard Lifecycle:** All telematics logs and associated video alerts are automatically and irreversibly deleted from our servers after **12 months**.
- **Extended Lifecycle Premium Tier:** Where explicitly authorized via commercial amendment, select accounts feature extended lifecycles of **15 or 24 months** before absolute system deletion.
- **Post-Termination Obligation:** Upon absolute termination of service contracts, all active platform records, custom placemarkers, and backup logs are purged from our live database arrays within **30 days**.

End Of Document