Overview House
Kingswey Business Park
Forsyth Road
Woking UK GU21 5SA

T: +44 208 875 0984
E: info@overview.co.uk

AUGUST 2026

STATEMENT ON NETWORK CONNECTIVITY AND DATA SECURITY

Following recent reports concerning connected camera systems transmitting telemetry or "heartbeat" data to external services, Overview Ltd have prepared the following statement to clarify how our PodView™ sensor system operates and why we do not think it has the same risks.

PodView is developed using a combination of Overview proprietary software and widely adopted industry-standard technologies, including commercially supported operating systems, NVIDIA software frameworks, and selected open-source components. Using established open-source software provides the benefit of transparency and continuous scrutiny by global developer and cybersecurity communities, helping to identify and address vulnerabilities more rapidly than may be possible with closed, proprietary software alone.

PodView's software is developed specifically to support the processing, management, and delivery of customer data within the customer's intended operating environment. When deployed within customer-managed networks and security architectures, PodView remains under the customers network controls, firewall policies, monitoring, and access management. Importantly, PodView does not require unrestricted internet connectivity for its core operational functions, and Overview recommends that deployments follow established cybersecurity best practice by restricting network access to only those services and destinations required for the intended application.

Like most modern computing platforms, the system incorporates a mixture of proprietary and third-party software components that are maintained through regular updates and security monitoring. While no complex software system can credibly claim zero cybersecurity risk, Overview is not aware of any functionality within PodView that is designed to communicate operational, image, customer or telemetry data to foreign governments or unauthorised third parties.

We continue to follow industry best practice in software maintenance, vulnerability management, and supply-chain awareness as part of our ongoing product security and assurance activities.