EROAD Group's Biometric Data Retention and Destruction Policy

Last updated: July 2025

EROAD's Clarity Edge dashcam and our auxiliary fatigue cameras ("Dashcams") utilize dashcam video together with advanced machine learning to help monitor driver behaviours such as distraction, yawning, continuous eye closure, frequent blinking, mobile phone usage, smoking, unfastened seatbelts and covered camera lenses, provided our customer obtains any required legal consent from drivers before utilising our products. Our customers are responsible for installing EROAD dashcams in their fleet vehicles and customers decide which drivers operate vehicles equipped with these Dashcams.

While Dashcams do not explicitly identify individuals, but simply analyse facial features, eye movement, or patterns related to body or face, this can involve the use, processing and storing of biometric data according to many data privacy laws. This data is handled strictly for purposes outlined in EROAD's Terms and EROAD's Privacy Policy and always in accordance with applicable legal requirements. The driver identification information generated by Dashcams must be used exclusively to manage safety-related events within the customer's fleet. For additional details about the Dashcams and recommended privacy practices, please see below.

Biometric Data Retention Period:

Personal data captured by the Dashcams for a specific driver is retained for up to 18 months by default. However, this retention period is configurable by customers, with retention options ranging from 3 to 36 months. After this period, all biometric details are permanently deleted.

Customers retain control over their employees' data in the EROAD platform. Employees who wish to request deletion of their biometric information outside these standard retention periods should contact their employer, who in turn can coordinate with EROAD.

Dashcam Driver Consent:

Many jurisdictions, including the United States (for example, Illinois, Texas, and the city of Portland), have passed laws that have notice and consent requirements for how companies use, share, and store biometric data that can be used to identify individuals. If you have drivers who reside or operate vehicles in these jurisdictions, these laws may apply to your use of Dashcams. The law in this area is changing rapidly. The information

provided here is not intended to be legal advice or a substitute for legal advice. Please contact your legal representative if you have any questions or concerns.

However, we strongly encourage our customers to incorporate a notice and consent process into their driver onboarding and to implement their own Biometric Data Policy. For our customers' convenience, we've included the following consent form example. Before using this example, customers should make sure the example works for their intended use of Dashcams.

Example Consent Form

Consent to Collection of Biometric Data

We use EROAD's hardware and software technology to manage our fleet and improve driver safety. The Dashcam feature will collect, store, and process information about your face for purposes of managing safety and driver behaviour events in the EROAD dashboard. The facial information used by the Dashcam may include biometric data regulated under applicable law. The facial information used by the Dashcam is processed using either the Amazon Web Services (AWS) or Microsoft Azure cloud-based software. The Dashcam information is retained until ***[****18 months or choose a shorter or longer period****]*** *after the information is collected, at which point the Dashcam information, including any biometric data, will be permanently deleted. More information about the Dashcam may be found at EROAD's website: https://www.eroad.com/privacy-policy/ .*

A copy of our Biometric Data Policy is available on request.

By signing below, you consent to EROAD's and ***[****insert company name****]****'s collection, use, disclosure, and storage of your biometric data as described above.*

Signature: _____

Name: _____

Date: _____