

## *OpenEyes Device Privacy Notice*

### **PRIVACY NOTICE**

*Last updated on August 2025*

This **Privacy Notice** describes the personal data that OpenEyes Insurance Agency, Inc. (“OpenEyes”, “we”, “us”, “our”) collects when you use the driver’s risk prevention system developed by OpenEyes (the “OpenEyes Device”), how we use it, with whom we share it, and your choices in connection with this.

**Note to our clients:** You are responsible for informing the drivers of vehicles in which the OpenEyes Device is installed and any recipients of reports from the OpenEyes Device of the terms of this Privacy Notice and for obtaining any consents as may be required for the data processing that OpenEyes does, including any consents as may be required for the sharing of information with the insurance companies, loss adjusters and third-party claims administrators (“TPA”).

### **OUR ROLE IN DATA PROCESSING**

To the extent the General Data Protection Regulation (“GDPR”), Regulation (EU) 2016/679, and the UK Data Protection Act 2018 (“DPA”) apply (collectively referred to in this Privacy Notice as “EU or UK data protection laws”), unless stated otherwise, the entity responsible for the collection and use (processing) of your personal data is OpenEyes Insurance Agency, Inc., the data controller. You may contact OpenEyes by emailing [support@openeyes-insurance.com](mailto:support@openeyes-insurance.com).

Where we are providing the OpenEyes Device on behalf of a client (i.e. your employer / fleet manager), the client is the data controller and we are the data processor, and process personal data pursuant to the client’s instructions. In such instances, please contact the client (i.e. your employer / fleet manager) with any inquiries or to exercise your privacy rights and we will work with the client to fulfill them pursuant to the client’s instructions.

### **PERSONAL DATA WE COLLECT, WHY AND FOR HOW LONG**

We collect personal data, which is information relating to you as an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly. As used in this Privacy Notice, “personal data” includes “personal information” and “personal data”, as such terms are defined under applicable data privacy laws.

Depending on the nature of your relationship with us, we collect personal data directly from you, automatically as you drive a vehicle in which the OpenEyes Device is installed, and from third-party sources as described below.

**If you are a fleet manager or otherwise employed by one of our clients in a non-driving capacity, this includes when you:**

- **Procure our services.** When your organization procures our services, we collect, from you, your *identifiers* (name, email address, telephone number) and your *professional or employment-related information* (position, company name). We use this information to allow your access into the OpenEyes dashboard; communicate with you and to facilitate the business

relationship between OpenEyes and the organization you represent. To the extent the EU or UK data protection laws apply, the legal basis for this processing is that it is necessary for the performance of a contract or to take steps to enter into a contract. We retain this information until instructed to delete it by our client.

- **Engage us as an Insurance Agency (US Only).** When you engage us to serve as your insurance agency, use the information collected through the OpenEyes Device to assess the level of risk associated with your fleet. Our human experts use this information to make determinations regarding potential insurance products that are applicable for you and the related premium / cost of such products. You acknowledge, and inform your drivers, that this assessment may include the risky driving of specific drivers and may include requirements for improving a specific driver's driving and/or taking disciplinary action against such driver, including the termination of their employment.

**If you are employed as a driver, we collect information from you:**

- We aggregate the data we collect automatically from the OpenEyes Device for benchmarking purposes, for internal analysis of alerts received and to improve our services. To the extent the EU or UK data protection laws apply, the legal basis for this processing is our legitimate interest in improving the OpenEyes Device. We maintain and use this data in deidentified form. We will not attempt to reidentify the data, unless it is necessary to determine whether our deidentification processes satisfy applicable data protection laws. OpenEyes may also use the personal data we collect as described in this section to comply with the law, to efficiently maintain our business, and for other limited circumstances as described in the **HOW WE SHARE YOUR PERSONAL DATA** section.

**If you are employed as a driver, we collect information from you (at the instruction of your employer as a data processor unless stated otherwise), including when you:**

- **Setup the OpenEyes Device.** When you setup the OpenEyes Device, we collect from you or your employer your *identifiers* (name, state, date of birth, VIN, and license plate number of the relevant vehicle), *sensitive information* (Driver's License number), and your *professional or employment-related information* (driver schedule). We also collect your motor vehicle driving record from the applicable state department of motor vehicle. We use this information to facilitate the setup of the OpenEyes Device, create and manage your driver profile, and to document your driving performance. To the extent the EU or UK data protection laws apply, the legal basis for this processing is the performance of a contract for the provision of the services to your employer. We use your identifiers to provide customer service support and maintenance. To the extent the EU or UK data protection laws apply, the legal basis for the processing of this information is that it is necessary for the performance of contract for the provision of the services to your employer.
- **Drive a vehicle equipped with the OpenEyes Device.** When you drive a vehicle equipped with the OpenEyes Device, the OpenEyes Device automatically collects your *visual information* (video recording), *geolocation information* (GPS location), and your *biometric*

*identifiers* (face geometry, iris scan) through an internal (in-cabin) and an external camera powered by OpenEyes' AI technology.

The *internal camera* collects your visual information (video recording) and your biometric identifiers (iris scan, face geometry) by monitoring your pupils and physiological characteristics, such as the location and distance between your mouth, eyes, and lips as well as your head position. **We do not use this information to identify the identity of the driver.** We use this information to: (i) assess, using our proprietary algorithm, whether a dangerous driving event has occurred (as explained in greater detail below); (ii) provide you with real-time alerts; (iii) determine that you are a driver (and not a passenger); (iv) determine the location of dangerous events; (v) help fleet managers (your employer) locate vehicles through the OpenEyes dashboard; (vi) improve the fleet's efficiency; (vii) investigate incidents; and (viii) secure lost or stolen assets. The OpenEyes Device also indicates whether a camera has been disabled or blocked.

The *external video camera* captures and monitors how you are driving, emphasizing excessive proximity to other cars, approaching pedestrians, deviations from the lane markers, and non-compliance with traffic signs or traffic lights. We use this information to: (i) monitor your driving performance and compliance with traffic regulations; (ii) provide you with real time alerts; (iii) assess, using our proprietary algorithm, whether a dangerous driving event has occurred; and (iv) help you improve your driving and avoid collisions with other vehicles, objects, or individuals while you drive.

The OpenEyes Device also collects telemetry information about how you drive, such as accelerations, decelerations, sharp turns, and hard breaking. We use this information to monitor your driving performance, provide you with real-time alerts, and to assess, using our proprietary algorithm, whether a dangerous driving event has occurred.

- **When your driving triggers a “dangerous event”**

A dangerous driving event is any unsafe driving scenario and includes situations such as when: (i) the driver is not looking at the road; (ii) the driver appears to be falling asleep; (iii) the driver is driving erratically (including too close to other vehicles); (iv) the driver commits a traffic violation (running a stop sign or red light); or (v) the driver causes or almost causes an accident (with another vehicle or otherwise). The OpenEyes Device determines whether an event is by attributing values to different variables and assigning a degree of risk to each variable, alone and in conjunction with other variables (for example closed eyes by itself; and closed eyes together with lane deviation, fast speed and neighboring vehicles).

If the OpenEyes Device determines that a dangerous event has occurred, it will inform you through an audio alert. The OpenEyes Device logs the fact that alerts have been triggered. At this juncture, the OpenEyes Device will also trigger the recording of a 30 second video (without audio) documenting the event. At the fleet manager's (your employer's) option this may be for videos from only the internal camera, only the external camera or from both, or may be triggered only in the event of an accident.

- **When you receive a “driver safety score”**

The OpenEyes Device attributes a driver safety score per vehicle based on the information collected throughout the driving of the vehicle. The driver safety is a weighted combination of the risky incidents within a large time window (usually weeks prior to the current time). The driver safety score is impacted by both risky incidents and actual accidents which have occurred within the time window and maps a score to each vehicle/driver ranging between 0 and 100 where 0 is very risky and vice versa. OpenEyes uses this information to make, to its clients, recommendations re enhancing driver training and coaching towards safer driving for its drivers. To the extent a vehicle is driven by a single driver, the safety score could be attributed to a specific driver. The client may, at its sole discretion, use the score as one of several factors used by its HR professionals in making disciplinary decisions regarding its drivers, up to and including termination of employment.

We share information with your employer (or fleet manager), service providers, insurance companies, loss adjusters and/or third-party claims administrators and other third parties, which can influence a client's (your employer or fleet manager) insurance rate or quote for new or additional insurance. How we share this information is further described in the **HOW WE SHARE YOUR PERSONAL DATA** section.

## **DATA RETENTION AND DESTRUCTION**

Both internal and external cameras of the OpenEyes Device record videos in ten-minute increments (or another increment as instructed by the fleet manager). Once the ten-minute increment is complete, the video deletes, and a new ten-minute increment commences. If within a given ten-minute increment, a dangerous event occurs (as explained below), if this option is selected by the fleet manager (your employer), a clip of such event is sent to the cloud (the length of the clip is configurable as instructed by the fleet manager and is generally in the order of tens of seconds). At the client's option, longer or continuous video footage may be retained.

OpenEyes will permanently delete biometric information upon the earlier of: (i) instruction by your employer / fleet manager to delete your biometric information; (ii) one (1) year (or a longer term if permitted by applicable law and instructed by our client) has passed since the last interaction between you and the OpenEyes Device, or (iii) the biometric information is no longer necessary for the purposes described in this Privacy Notice unless required a valid warrant or subpoena issued by a court of competent jurisdiction. In this context: you are considered to be "interacting" with the OpenEyes Device as long as you keep driving a vehicle equipped with the OpenEyes Device. Biometric information is considered necessary for purposes like: (i) whether there is a retention period required by statute or regulations; (ii) the existence of actual or threatened litigation for which we are required to preserve the information; (iii) the statutes of limitations for potential legal claims; and (iv) generally accepted best practices in our industry, including in relation to the safety and security of our properties and assets.

Unless otherwise stated in this Privacy Notice, we retain your personal data (i) for as long as there is a record/account of you with us, (ii) until we receive a valid request to delete the information, in which case we will delete or anonymize the information within thirty (30) days after receiving the request, (iii) until we no longer need the information to fulfill the purposes for which we

collected it, or (iv) until the information is no longer needed for a service provider or contractor's operational purpose(s).

We use the following criteria to determine whether it remains reasonably necessary to retain your personal data for such purposes or a service provider or contractor's operational purpose(s): (i) whether there is a retention period required by statute or regulations; (ii) the existence of actual or threatened litigation for which we are required to preserve the information; (iii) the statutes of limitations for potential legal claims; and (iv) generally accepted best practices in our industry, including in relation to the safety and security of our properties and assets. When we determine that it is no longer reasonably necessary to retain your personal data for one or more disclosed operational purposes based on the above criteria, we will delete or anonymize your personal data.

## HOW WE SHARE YOUR PERSONAL DATA

### General Sharing:

OpenEyes shares personal data in the following instances:

- **With the fleet manager (your employer, our client):** Your employer has access to the OpenEyes dashboard from which they can see: your identifiers (driver name, Driver's License number, and state), motor vehicle record; insurance policy information; log of dangerous events and their location; log of accidents and their location, videos of dangerous events and accidents as well as additional aggregated data on dangerous events logged by the OpenEyes Device. We share this information to provide the core services to our clients, including fleet management, driver coaching, and safe driving improvements.
- **With insurance companies and claims settlers:** If an insurance claim is filed in connection with an event or an accident, we share with the insurance company and/or claims settlers: your identifiers; insurance policy information, location and videos of accidents, longer videos of driving footage if such are retained by our client, as well as additional aggregated data on risky events logged by the OpenEyes Device for the purpose of informing the handling of claims and terms of existing or new policies and/or renewal of insurance.
- **With loss adjusters:** If an insurance claim is filed in connection with a dangerous event or an accident, we share with loss adjusters: your identifiers (name, Driver's License number, and state), GPS location, date and time of the accident or dangerous event, and the video of the accident or dangerous event. We share this information to assist the loss adjuster with processing the claim.
- **With service providers:** We share your personal identifiers (name, Driver's License number, and state), GPS location, and video of you during a dangerous event or accident, with our service providers that assist us in providing the OpenEyes Device. These service providers include, IT support, cloud storage providers, communications providers, claims TPAs, and analytics providers. We share this information to provide our services to our clients and insurance carriers.

- **Within OpenEyes' corporate family:** We share your personal data within our organization for legitimate business purposes including improving our OpenEyes Device, general business management, and as permitted by law. To the extent the EU or UK data protection laws apply, the legal basis for this is our legitimate interest in providing the OpenEyes Device more efficiently or, if required by law, consent.
- **In the event of a corporate reorganization:** In the event that we enter into, or intend to enter into, a transaction that alters the structure of our business, such as a reorganization, merger, acquisition, sale, joint venture, assignment, consolidation, transfer, change of control, or other disposition of all or any portion of our business, assets or stock, we would share personal data with third parties, including the buyer or target (and their agents and advisors) for the purpose of facilitating and completing the transaction. We will also share personal data with third parties if we undergo bankruptcy or liquidation, in the course of such proceedings. To the extent the EU or UK data protection laws apply, the legal basis for this is our legitimate interest in carrying out our business operations or, if required by law, consent.
- **For legal purposes:** We will share personal data where we are legally required to do so such as in response to court orders and/or subpoenas, law enforcement, or legal process, including for national security purposes; to establish, protect, or exercise our legal rights, as required to enforce our terms of service or other contracts; to defend against legal claims or demands; or to comply with the requirements of any applicable law. To the extent the EU or UK data protection laws apply, the legal basis for this processing is compliance with the law or our legitimate interest in complying with non-EU data protection laws to which we are subject.
- **With your consent:** Apart from the reasons identified above, we may request your permission to share your personal data for a specific purpose. We will notify you and request consent before you provide the personal data or before the personal data you have already provided is shared for such purpose. You may revoke your consent at any time with effect going forward by emailing us at [support@openeyes.com](mailto:support@openeyes.com).

### **Sharing of Biometric Information:**

We share your biometric identifiers (iris scan, face geometry) (as such as defined under US biometric laws) only with our cloud storage provider for the purpose of data storage. We do not sell, lease, exchange, or trade any biometric identifiers or biometric information.

As required by US biometric data law, OpenEyes will not disclose, disseminate, and/or transmit any of your biometric identifiers or biometric information to any person or entity other than to our cloud storage provider without/unless:

- First having obtained your written consent or that of your legally authorized representative;
- The disclosed information completes a financial transaction authorized by you or by your legally authorized representative;
- Disclosure is required by state or federal law; or
- Disclosure is required pursuant to a valid warrant or subpoena.

## **RIGHTS OF INDIVIDUALS IN THE EU OR UK:**

Individuals in the European Union and United Kingdom are entitled to certain rights under General Data Protection Regulation (“**GDPR**”) and the Data Protection Act 2018 (“**DPA**”), respectively. The Texas Data Privacy and Security Act (“**TDPSA**”) also entitles Texas residents to certain rights. To the extent these laws apply to our processing of your personal data, you are entitled to the following rights. These apply to our processing of personal data as a data controller. Where we process the data as a data processor, please contact the client (i.e. your employer / fleet manager) with any inquiries or to exercise your privacy rights and we will work with the client to fulfill them pursuant to the client’s instructions

- **Right to access:** For any of the processing described above, you have the right to ask us for copies of your personal data. However, this right has some exemptions, which means you may not always receive all the personal data we process. Applicable exemptions may include the management information exemption (data that we process for management forecasting or management planning about a business or other activity), or certain instances of ongoing or prior negotiations with the requestor, among others.
- **Right to rectification/correct:** For any of the processing described above, you have the right to ask us to rectify personal data you think is inaccurate or incomplete.
- **Right to erasure/deletion:** You have the right to ask us to erase your personal data with certain exceptions. In the EU/UK, one such exception is when the legal basis for the processing is to fulfill our legal obligations or to carry out a task in the public’s interest. In Texas, for example, if we are required by law to retain the information that you are asking to be deleted, we would not be able to delete the information until we are legally permitted to delete it.
- **Right to data portability:** You have the right to ask that we transfer the personal data you gave us from one organization to another or give it to you. However, in the EU/UK this right only applies when: (i) you have provided your personal data to us; (ii) the legal basis for the processing is your consent or for the performance of a contract; and (iii) the processing is carried out by automated means. You can invoke this right for the processing of the information connection with your account information.

If GDPR or the DPA applies to our processing of your personal data, you are also entitled to:

- **Right to restrict processing:** For any of the processing described above, if you believe that your personal data is inaccurate, that our processing is unlawful, or that we do not need your personal data for a specific purpose, you have the right to request that we restrict the processing of this personal data. You also have the possibility to request that we stop processing your personal data while we assess your request. If you object to our processing (per your right to object below), you may also request us to restrict processing of your personal data while we make our assessment.

- **Right to object to processing:** You have the right to object to our processing of your personal data when the legal basis for the processing is pursuant to our legitimate interests by referencing your personal circumstances.
- **Right to lodge a complaint:** If you are located in the UK, you have the right to lodge a complaint with the Information Commissioner’s Office at: <https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/y> or [accessicoinformation@ico.org.uk](mailto:accessicoinformation@ico.org.uk) at their helpline on 0303 123 1113. If you are located in the EU, you have the right to lodge a complaint with the relevant [Supervisory Authority](#).

If TDSPA applies to our processing of your personal data, you are also entitled to:

- **Right to Non-Discrimination.** You have the right to not receive discriminatory treatment in the processing of your personal data if you choose to exercise your privacy rights under the TDPSA.
- **Right to Appeal.** You have the right to appeal an action taken (or not taken) by OpenEyes in response to your request. We will inform you of any action we have taken in response to your request without delay and, in any event, within forty-five (45) days after we receive your request. To exercise your right to appeal, you may submit your appeal by emailing [support@openeyes.com](mailto:support@openeyes.com). If you are a concerned with our response as a result of your appeal, you may submit a complaint to the Texas Attorney General [here](#).

If you wish to exercise your privacy rights, you may submit your request to [support@openeyes.com](mailto:support@openeyes.com).

For requests submitted via telephone, you must provide us with sufficient information that allows us to reasonably verify you are the person about whom we collected the personal data and describe your request with sufficient detail to allow us to properly evaluate and respond to it. In doing so, we will take steps to verify your request by matching information provided by you with the information we have in our records. If we are not able to verify your identity for access and deletion requests with the information provided, we may ask you for additional pieces of information.

Only you, or a person that you authorize to act on your behalf may make a request related to your personal data. If you are an authorized agent making a request on behalf of another individual, you must provide us with signed documentation that you are authorized to act on behalf of that individual.

Where we are providing the OpenEyes Device on behalf of a client (i.e. your employer / fleet manager), to exercise your rights, you will need to submit your request to the client directly. We will assist the client in fulfilling your request to the extent we are legally or contractually obligated required to.

## NEVADA RESIDENTS

If you are a consumer in the State of Nevada, you may request to opt-out of the current or future sale of your personal data. We do not currently sell any of your personal data under Nevada law, nor do we plan to do so in the future. However, you can submit a request to opt-out of future sales by contacting us at [support@openeyes.com](mailto:support@openeyes.com) regarding the sale of such information. Please include “Opt-Out Request Under Nevada Law” in the subject line of your message.

## **INFORMATION SECURITY**

We implement and maintain reasonable security measures, such as access controls, multi factor authentication, encryption, separate storage environments for clients, firewall, to protect the personal data we collect and maintain from unauthorized access, destruction, use, modification, or disclosure. However, no security measure or modality of data transmission is 100% secure and we are unable to guarantee the absolute security of the personal data we have collected from you.

With respect to biometric Information/Identifiers (as defined by US biometric data laws): OpenEyes uses and requires its service providers who store or have access to biometric information to use, a reasonable standard of care to store, transmit and protect from disclosure any biometric information collected. Such storage, transmission, and protection from disclosure is performed in a manner that is the same as or more protective than the manner in which OpenEyes stores, transmits, and protects other confidential and sensitive information, including personal data.

## **CHILDREN’S PRIVACY**

The OpenEyes Device is not intended for individuals under the age of eighteen (18) years. If we learn that we have collected or received personal data from individuals under the age of eighteen (18), we will delete the personal data. If you believe we have personal data on individuals under the age of eighteen (18), please contact us at the contact information provided below.

## **CROSS-BORDER TRANSFERS**

We, as well as some of our service providers that process personal data in connection with the OpenEyes Device are located in countries outside of the European Economic Area (EEA) and United Kingdom that have not been found by the European Union nor the United Kingdom Secretary of State to provide an adequate level of protection of personal data, i.e. a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union or United Kingdom and where your personal data may be accessible to law enforcement or other authorities pursuant to a lawful request. To carry out such transfers in compliance with EU and UK data protection laws, we have put in place appropriate safeguards to protect the personal data that is transferred to, stored and/or processed in other countries, by contractually obligating our service providers to adhere to the terms of a data processing agreement, which incorporates the EU Standard Contractual Clauses (as applicable), and UK Addendum.

## **CHANGES TO THIS PRIVACY NOTICE**

This Privacy Notice is subject to change. Changes to the Privacy Notice will be posted on this page and we will indicate the date the changes go into effect. We encourage you to review this page frequently and review the Privacy Notice for any changes. If we make changes that materially affect your privacy rights, we will notify whomever (i.e. our client / your employer or fleet manger) maintains the obligation to notify you of your rights described in this Privacy Notice. If we have sufficient information, we may notify you by email and obtain your consent if required by law.

## **CONTACT US**

If you have any questions or concerns regarding this Privacy Notice, please contact us at [support@openeyes.com](mailto:support@openeyes.com).