

# Guardian Privacy Notice

---

Seeing Machines Limited and its wholly-owned subsidiaries (the Seeing Machines Group), a global group of companies headquartered in Australia, are an industry leader in computer vision technologies, which enable machines to see, understand and assist people.

The Seeing Machines Group has developed Guardian, an intelligent driver monitoring system. This privacy notice aims to help you understand how we protect and manage personal data/information relating to Guardian. It focuses on the personal data that we collect and process to provide the Guardian product and services to our clients and distributors, including support provided by authorised third-parties, that may install, maintain, and/or support our products and services.

The European Union has implemented a privacy and security framework called the [General Data Protection Regulation](#) (GDPR). This document provides you with information as required under [Articles 13](#) and [14](#) of the GDPR, as well as meeting the requirements of the [Australian Privacy Act 1988](#) (Cth) and the [Australian Privacy Principles](#).

## 1. Why is the General Data Protection Regulation important?

The GDPR imposes obligations about how organisations, such as the Seeing Machines Group, collects and manages personal data. It provides European Union (EU) Citizens with a range of rights relating to their personal data, including access and deletion rights, regardless of where the data is located in the world. Under the GDPR, organisations have different responsibilities, depending on their role. For example, a “[data controller](#)” is responsible for determining the purpose and means of processing personal data, whereas a “[data processor](#)” is responsible for managing personal data according to instructions from the “data controller”.

## 2. Who we are?

We build image-processing technology that tracks the movement of a person's eye, face, and head. We incorporate this technology into products and services for a range of industries, including Guardian products and services. Our products capture and generate data about driver (or operator) performance (including fatigue and distraction) and transmit that data (including personal data) to our Guardian Center (monitoring center), where we review events detected by Guardian. This enables our clients and distributors to monitor and manage their drivers and fleet.

Our principal places of business are:

- Canberra, Australian Capital Territory, Australia
- Tucson, Arizona, United States of America
- London, England, United Kingdom

Our GDPR representative within the EU is:

Seeing Machines (UK) Ltd  
Company number: 10746642  
c/o Fieldfisher, Riverbank House, 2 Swan Lane, London, EC4R 3 TT, England,  
United Kingdom

Individuals wishing to contact us about data protection issues may reach us via our Privacy & Data Protection Officer:

**via e-mail** at [privacy@seeingmachines.com](mailto:privacy@seeingmachines.com) or

**via mail** at:

Att: Privacy & Data Protection Officer  
Seeing Machines Limited  
80 Mildura Street,  
Fyshwick, ACT, 2609

Under the GDPR, we are a “[data processor](#)” or “sub-processor” to the extent that we collect and manage personal data about EU citizens on behalf of our Guardian clients and distributors. In these circumstances, our clients are considered “[data controllers](#)” and we process personal data according to contracts and written instructions from them as data controllers and/or our distributors as data processors.

### 3. What kinds of personal data might we hold about you?

We collect and manage personal data relating to the employees, contractors and agents of our clients, distributors, partners and authorised third-parties.

We primarily obtain personal data about our client’s employees and contractors as a result of providing Guardian products and services, such as personal data in the form of in-vehicle video recording and images of the driver. We may also collect other personal information if a client provides us with personal data about their drivers, such as names and identification numbers, so it can be matched up with vehicle monitoring data to enable the client to better manage their fleet. The categories of personal data that we may collect relating to our clients’ employees and contractors include:

- information about the performance of client’s employees and contractors (e.g. video and still—images of the driver, as well as images from a forward-facing camera),
- information about the drivers’ behavior through fatigue and distraction events,
- other fleet of vehicle monitoring information (e.g. GPS coordinates, shift times, or vehicle speed),
- contact information (e.g. telephone number for a client’s contact officer to notify about fatigue events, driver’s location, company name and contact details),
- identification information (e.g. driver name, driver unique identifier, vehicle identifier),
- electronic identification information (e.g. email, internet protocol (IP) addresses, browser type, internet service provider (ISP)), system usage and preferences when our clients’ employees, sub-contractors and agents accesses on-line services, reports or other electronic information.

This data is kept in its identifiable form so that Guardian clients and distributors can monitor driver fatigue and distraction, prevent accidents, and manage their vehicles or fleet. This data is also grouped and de-identified to provide reports for our clients and distributors. We may also use this data for scientific research to enhance, improve, or modify our products and services or to help develop new products and services.

In collecting this information, we may also obtain special category (sensitive) personal data about our client’s drivers, as [defined by Article 9 of the GDPR](#), such as, data revealing racial or ethnic origin or data concerning a person’s health. This data is obtained as a result of in-vehicle video recording and images of the driver or operator and information about the drivers’ driving behavior, such as fatigue and distraction events, but we do not record racial, ethnic or health data in our Guardian databases.

In addition, our distributors, partners and affiliates may provide us with personal data about their employees, contractors or agents, in order for us to provide them with access to our systems, training, certification, technical information and other services. For example, a distributor may provide us with their installers, names, identification numbers and contact details, so that they can log-into our installation training and become accredited as a Guardian installer. The categories of personal data that we may collect in relation to our distributors’, partners, and authorised third-parties are:

- identification information (e.g. account manager’s name for services, such as product installation or fleet monitoring; unique employee identifier),
- contact information (e.g. account manager or installers’ telephone numbers, emails, locations),

- information on the performance of the distributor’s employees, contractors or agents, and /or authorised third-parties, such as contracted installers (e.g. training accessed, certification),
- electronic identification information (e.g. email, internet protocol (IP) addresses, browser type, internet service provider (ISP)), system usage and preferences when an individual accesses on-line services, training or information.

This data is kept in its identifiable form to enable access to: facilitate installation, configuration, testing, operation, warranty, repair and maintenance of our products and services; our systems, training, certification, information products, and support services; and respond to inquiries, send notices, resolve disputes, and troubleshoot problems. This data is also processed in a de-identified form to provide reports for our distributors, partners and authorised third-parties. We may also use this data for scientific research to enhance, improve, or modify our products and services or to help develop new products and services.

#### 4. What authority do we have to collect or process your personal data?

We collect and process your personal data under the authority and direction of our clients (the data controllers), distributors, partners and authorised third-parties (data processors), in accordance with [Article 29 of the GDPR](#). In most instances, the basis for this is either consent provided by you to your employer or contractor (whether our client or distributor) or under your employment contract, in accordance with [Article 6\(1\)\(a\) or \(b\) of the GDPR](#).

Where we retain and use your personal data (in both identifiable and aggregate form) in order to enhance, improve, or modify our products and services or to help develop new products and services, we do so, based on our legitimate commercial and scientific interests, in accordance with [Article 6\(1\)\(f\) of the GDPR](#). Those interests are to develop an understanding of the real-world safety behaviours of drivers to design technology to address these behaviours to help make the world a safer, smarter place for drivers and the wider community.

#### 5. What do we do with your personal data?

We collect and process your personal data to provide Guardian products and services. This personal data is used to:

- detect, diagnose and mitigate driver or operator fatigue or distraction, and other dangerous driving events,
- enable configuration, testing, operation and maintenance of the Guardian system,
- to provide technical support to our clients and distributors, for example to enable repair of an in-vehicle recording device,
- provide aggregate reports or information on specific driver or vehicle events, such as an accident, which may include video recordings of drivers or operators,
- for our business purposes, such as: data analysis; audit; fraud monitoring and prevention; to enhance, improve, or modify our products and services; employee training; and operating and developing new products and services,
- for scientific research to enhance, improve, or modify our products and services or to help develop new products and services.

Any personal data that we collect will be processed strictly in accordance with contractual instructions from our clients and distributors.

#### 6. Who do we share your personal data with?

We share your personal data with:

- your employer (our clients, distributors, partners and authorised third-parties) to enable them to detect, diagnose and prevent driver and operator fatigue, distraction, and other dangerous driving events,
- our distributors, partners and authorised third-parties, for Guardian configuration, testing, operation and maintenance and support purposes,

- third-parties, as authorised or directed by our clients, such as telematics providers (data analysts) who combine your personal data with other vehicle or fleet monitoring information to provide reports or services to these clients,
- contracted third-parties that collect or process personal data on our behalf, such as Amazon Web Services that hosts our Guardian data base,
- authorised third-parties in connection with our business activities, such as external auditors, insurers or any organisation that might be appointed in respect to a merger or sale of our business.

We may disclose your personal data to other entities for the purposes described above and with another entity in order to comply with our obligations under relevant jurisdictional law. We will do this: when the law requires it; at the direction of a government authority; in responding to an emergency, declared by a State, Territory, Federal or National Government (see [DiasterAssist](#) for declared Australian Emergencies); for national security, law enforcement or litigation purposes; or in the event we sell or transfer all or a portion of our business or assets.

We will not share or sell your personal data with unaffiliated third-parties for any other purpose.

## 7. What data protections do we use?

We take great care to handle personal data consistent with data protection laws and according to the contracts or written instructions from our Guardian clients (the data controllers) and our distributors (data processors). The Seeing Machines Group uses the following mechanisms to protect your data:

- active management of data access – only those who need access to personal data in order to provide or support the provision of those products or services, have access to that data, with both physical and IT access restricted for different users based on user/access rights models,
- secure log on and access– our IT systems utilise strength-tested passwords and unique identifiers and our premises have secure key card access,
- logging – within our IT systems, there is tracking of certain activities, based on specific user roles and the activities,
- IT system maintenance – our IT systems are constantly monitored and maintained, with telemetry in place to track upgrades and bugs,
- IT system protections – our systems use industry standards to protect personal data and we rely on those systems security to protect your data, with most systems including protection from and monitoring for malicious software,
- physical protections – archived data is stored within secure on-site servers,
- contractual restrictions – use of data by third-parties, such as our contracted IT system providers, is limited to the allowable uses set out in contracts and as governed by relevant data protection laws,
- training and approvals – our employees who access personal data have been made aware of data protection and privacy requirements, with key employees being authorised and receiving specialist training. In addition, all employees have signed confidentiality agreements.

We use reasonable organisational, technical, and administrative procedures designed to protect Personal Data. Unfortunately, no system, data transmission or storage mechanism can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us in accordance with the “Contacting Us” section.

## 8. How long do we retain your personal data?

Our general data retention cycle means that we usually keep your personal data for 12 months, to provide Guardian products and services. However, in some instances, our client or distributor contracts or jurisdictional law may require data retention for a different timeframe. As agreed with our clients and distributors, we may retain your data for longer for scientific research to enhance,

improve, or modify our products and services or to help develop new products and services. In these circumstances, access to your data is tightly controlled.

Personal data that is not used is deleted. If you object to us processing your data, we will remove it from our systems in accordance with our data deletion cycle, unless we have a valid justification to hold on to it, such as to resolve disputes or comply with our legal obligations.

## 9. Do we transfer your data?

Access to your personal data predominately occurs within the Guardian database, which resides within a system provided by Amazon Web Services in the United States. Information about the EU—US Privacy Shield Framework may be accessed here: [www.privacyshield.gov](http://www.privacyshield.gov).

When required, we may transfer personal data in accordance with the European Commission-approved Standard Contractual Clauses, a copy of which can be obtained at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087>. Your personal data will not be transferred unless a valid transfer mechanism is in place legitimising such a transfer. Safeguards afforded by the EU model clauses may be accessed here: [https://ico.org.uk/media/1571/model\\_contract\\_clauses\\_international\\_transfers\\_of\\_personal\\_data.pdf](https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf)

## 10. What are your rights?

Individuals have a number of rights under the GDPR and similar data protection laws. Should you wish to exercise those rights, in the first instance, please speak to your employer or contractor. Otherwise you may contact us:

**via e-mail** at [privacy@seeingmachines.com](mailto:privacy@seeingmachines.com) or

**via mail** at:

Att: Privacy & Data Protection Officer  
 Seeing Machines Limited  
 80 Mildura Street,  
 Fyshwick, ACT, 2609

In the event of a complaint, you may also contact the relevant supervisory authority in your country.