SEEING MACHINES GROUP DATA PROTECTION AND PRIVACY POLICY

1. INTRODUCTION

Seeing Machines Limited is headquartered in Australia and is the parent company for a number of wholly-owned subsidiaries (the Seeing Machines Group). We are an industry leader in computer vision technologies, which enable machines to see, understand and assist people. We harness human factors science to create artificial intelligence technology that observes a driver's attention – reliably, unobtrusively, and in real time – and intervenes seamlessly when necessary. We use data to develop an understanding of the real-world safety behaviours of drivers, pilots and other vehicle operators, and we design human sensing technology to address these behaviours in order to help make the world a safer, smarter place for drivers and the wider community.

Our image-processing technology tracks the movement of a person's eye, face, and head. We incorporate this technology into products and services for a range of industries, such as automotive, fleet, aviation and rail. Our products capture and generate data about driver, pilot and operator performance (including fatigue and distraction events) and transmit this data (including Personal Data) to our monitoring centre. We process this data to enable our clients and distributors to monitor and manage their drivers, for example, by monitoring truck driver fatigue to reduce the risk of accidents. Our distributors and authorised third-parties also have a role in selling, installing, maintaining, and supporting our products and services. To fulfil these roles, they access a range of information, including Personal Data.

We respect the privacy of individuals and are committed to protecting the Personal Data we collect and manage in accordance with this policy, relevant data protection legislation, our contracts, and our stakeholders' expectations.

2. SCOPE

This policy applies globally to all Personal Data under the control of the Seeing Machines Group or our employees as a result of their work. It does not apply to other entities outside of our control (i.e. distributors or clients) or to the Personal Data of Seeing Machines' employees, directors, officers, and applicants. We have a separate policy covering the Personal Data of our employees, officers, directors, and applicants.

Under Article 4 of the *General Data Protection Regulation* (GDPR), Personal Data means "…any information relating to an identified or identifiable natural person….an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The *Australian Privacy Act 1988* (Cth) has a similar, although slightly broader definition of personal information, which includes "…information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not".

Recognising both of these definitions, for the purpose of this policy, Personal Data means any information, including an opinion (whether true or not), about an individual whose identity is identified or can reasonably be identified. Examples of Personal Data are: names; home addresses, including email addresses; referees reports; photos and video images; and telephone numbers or other individual contact information.

3. PURPOSE

This policy provides information on how we manage Personal Data, as required under Australian Privacy Principle 1.3 and in accordance with Australian Privacy Principle 1.4. It also provides information about the collection and processing of Personal Data, as required under Articles 13 and 14 of the GDPR.

The GDPR imposes obligations about how organisations, such as the Seeing Machines Group, collects and manages the Personal Data of European Union (EU) Citizens, regardless of where they are in the world. 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.

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 clients and distributors. Our clients are "data controllers". In these circumstances, we process personal data according to contracts and written instructions from our clients (the data controllers) and/or our distributors (data processors). However, where we collect information directly, such as Personal Data from individuals visiting our premises or website, we are a "data controller" and have additional responsibilities in how we collect and process that data.

4. RELEVANT DATA PROTECTION LEGISLATION

As an international Australian based company with employees located around the globe, we must comply with relevant jurisdictional data protection legislation, including but not limited to the:

- *Australian Privacy Act 1988* (Cth) (the Privacy Act);
- *Information Privacy Act 2014* (ACT);
- General Data Protection Regulation (GDPR);
- Arizona Revised Statue HB2154,13-3001, 18-551 and related statue; and
- United Kingdom Data Protection Act 2018 (UK).

5. COLLECTION OF PERSONAL DATA

In providing Seeing Machines' products and services, we collect and manage a range of data from different sources, including Personal Data about: our clients' employees, contractors or agents; our distributors' employees, contractors or agents; our suppliers' employees, contractors or agents; other end users of our products and services; potential investors for marketing purposes; individuals, through digital services, such as social media or newsletters; and individuals that interact with us or our employees, such as by visiting our premises or phoning our staff. The categories of Personal Data that we may collect is identified in table 1 below.

Table 1: Personal Data that may be Collected by the Seeing Machines Group

Data subject	Categories of Information	Purpose	Legal Basis	Our Role
Our client's employees or contractors	• Identification information (e.g. contact officer name for services, such as product installation or fatigue event notification; name; unique employee identifier; vehicle identifier). • Contact information (e.g. telephone number for a client's contact officer to notify about fatigue events, email, location, company name). • Information about the performance of our client's employees, including drivers or operators (e.g. video and still-images of the driver, as well as images from a forward-facing camera)[1]. • Information about the drivers' driving behavior (e.g. fatigue and distraction events). • Other fleet or vehicle monitoring information (e.g. GPS coordinates, shift times, or vehicle speed). • Internet service provider (ISP), system usage and related preferences, if our clients' employees and sub-contractors accesses on-line services, reports or other electronic information.	To: ○ provide services to clients to detect, diagnose and mitigate driver fatigue or distraction, and other dangerous driving events, ○ enable configuration, testing, operation, warranty, repair and maintenance of our products and services, ○ provide reports to clients and distributors on specific driver or vehicle events, including video recordings of drivers or operators, ○ provide summary reports for clients and distributors, such as event duration or distance trends, ○ respond to inquiries, send notices, resolve disputes, and troubleshoot problems, ○ undertake our ongoing business operations, such as audit, fraud control or financial management, ○ enhance, improve, or modify our products and services, including for scientific research.	• Performance of contract. • Agreement and consent of individuals. • Legitimate interest: ○ manage the relationship with and provide services to our clients, ○ delivery of training and/or certification, ○ communications, ○ improvement of our business processes, services and products, ○ scientific research, ○ compliance with legal obligations. • To safeguard our legitimate interests or that of a third party, so long as fundamental rights and freedoms are protected. • Activities essential for protecting vital interests of individuals (for example in an emergency).	Data Processor

[1] In collecting this information, we may also obtain sensitive Personal Data about our client's employees, as defined by Article 9 of the GDPR or clause 6 of the Privacy Act, such as, biometric data (i.e. facial images), 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 databases.

Our distributors' and authorised third-parties' employees and contractors	• Identification information (e.g. installers name for services, such as product installation scheduling; unique employee identifier). • Contact information (e.g. telephone number, email, location, company name). • Information on the performance of their employees (e.g. training accessed, certification). • Electronic identification information, internet service provider (ISP), system usage and related preferences, email address, when they contact us, undertake training, lodge a ticket, or access on-line services or information.	To: ○ enable them to manage end-to-end client relationships including providing technical and support services, ○ enable installation, configuration, testing, operation, warranty, repair and maintenance of Seeing Machine's products and services, ○ enable access to our systems, training, certification, information products, and support services, ○ respond to inquiries, send notices, resolve disputes, and troubleshoot problems, ○ undertake our ongoing business operations, such as audit, fraud control or financial management, ○ enhance, improve, or modify our products and services, including for scientific research.	• Performance of contract. • Agreement and consent of individuals. • Legitimate interest: ○ invoicing, sales and logistics, ○ marketing activities, ○ delivery of training and/or certification, ○ manage the relationship with and provide services to third parties, ○ communications, ○ improvement of our business processes, services and products, ○ scientific research, ○ compliance with legal obligations. • To safeguard our legitimate interests or that of a third party, so long as fundamental rights and freedoms are protected. • Activities essential for protecting vital interests of individuals (for example in an emergency). • Auditing and financial management.	Data Processor or Controller depending on our' control over activities.

Our suppliers', their employees and contractors	• Identification information (e.g. account manager's name for services). • Contact information (e.g. telephone number, email, location [including home office information], company name). • Financial information, such as bank account details to enable payments (while usually company bank accounts, this may include Personal Data in certain instances such as sole traders). • Electronic identification information, internet service provider (ISP), system usage and related preferences, email address, when they contact us, access on-line services or information.	To: ○ facilitate the provision of services to Seeing Machine's, such as supply of IT equipment, ○ manage our contracts, ○ respond to inquiries, send notices, resolve disputes, and troubleshoot problems, ○ undertake our ongoing business operations, such as audit, fraud control or financial management, ○ enhance, improve, or modify business processes.	• Performance of contract • Legitimate interest: ○ invoicing, sales and logistics, ○ management of the relationship, ○ communications, ○ improvement of our business processes, services and products, ○ compliance with legal obligations.	Data Processor or Controller depending on our' control over activities.
Individuals who engage with us in relation to marketing or corporate communication	• Identification information (e.g. name). • Contact information (e.g. email address, telephone number, company name). • Electronic identification information, internet service provider (ISP), system usage and reeled preferences, and email address, when they contact us, or access on-line information.	To: ○ inform individuals and organisations about our activities, including sending our newsletters or reports, ○ facilitate our activities as a public company, such as continuous disclosure, ○ respond to inquiries, send notices, resolve disputes, and troubleshoot problems, ○ undertake our ongoing business operations, such as audit, fraud control or financial management, ○ to ensure that content from our site is presented in the most effective manner for the individual and their computer.	• Consent (i.e. newsletters, mailing lists). • Legitimate interest (i.e. to manage the relationship, the improvement of our business processes, marketing activities, communication, for any developments related to corporate restructuring).	Data Controller

Shareholders, board members and individuals who engage with Seeing Machines in relation to investment, or other corporate engagement	• Share-holding related information, such as share offers and/or transactions (including in limited circumstances contact information). • Conflict of interest information in relation to board members. • Biographical information in relation to board members. • Electronic identification information, internet service provider (ISP), system usage and related preferences, and email address, when they contact us, or access on-line information.	To: ○ inform individuals and organisations about our corporate or shareholding activities, ○ facilitate our activities as a public company, including maintaining our share register and communicating with shareholders, ○ respond to inquiries, send notices, resolve disputes, and troubleshoot problems, ○ meet our corporate governance, shareholder, trading, disclosure and related obligations, ○ undertake our ongoing business operations, such as audit, fraud control or financial management, ○ to ensure that content from our site is presented in the most effective manner for the individual and their computer.	• Consent (i.e. newsletters, mailing lists) • Legitimate interest (i.e. to manage the relationship, the improvement of our business processes, to provide financial and/or performance reports, for any developments related to markets and/or corporate restructuring).	Data Controller
Individuals who visit our premises	• Identification information (e.g. name). • Contact information (e.g. address, telephone number). • Video and still-images of visitors to our premises.	To: ○ maintain the safety and security of our premises, information and assets, ○ to meet our legal obligations, such as those relating to health and safety.	• Legitimate interest (i.e. security of our premises, the improvement of our business process, communications; to meet our legal obligations).	Data Controller
Individuals who engage with our corporate digital services (i.e. visit our website) or email or telephone our employees	• Identification information (e.g. name). • Contact information (e.g. email address, telephone number). • Electronic identification information, internet service provider (ISP), system usage and related preferences, and email address, when they contact us, or access on-line information.	To: ○ to ensure that content from our site is presented in the most effective manner for the individual and their computer, ○ respond to inquiries, send notices, resolve disputes, and troubleshoot problems, ○ undertake our ongoing business operations, such as audit, fraud control or financial management.	• Legitimate interest (i.e. security of our systems, the improvement of our business process, communications; to meet our legal obligations).	Data Controller

6. SHARING PERSONAL DATA

We may disclose 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 Personal Data with unaffiliated third parties for any other purpose.

7. RETENTION OF PERSONAL DATA

We retain Personal Data about a range of individuals in order to provide our products and services. For example, we retain Personal Data, in the form of in-vehicle video recording and images of drivers, for 12 months to enable our clients to monitor driver fatigue and distraction and therefore prevent accidents. Overall, we retain Personal Data for the minimum period required to achieve the purposes outlined in this policy (see Table 1), unless a different retention period is required under our client or distributor contracts or relevant jurisdictional legislation. We may also retain certain Personal Data related to our products and services for longer in order to enhance, improve, or modify our products and services or to help develop new products and services. In these circumstances, access to that Personal Data is tightly controlled.

Personal Data that is not used for any purpose is deleted. If a person objects to us processing their Personal 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.

8. PERSONAL DATA RIGHTS

With your assistance, we aim to ensure that the Personal Data that we collect and process, is accurate, up-to-date, complete and relevant. Individuals have the following rights with regards to their Personal Data.

- **Opt-out of our use of Personal Data**
  Individuals may withdraw consent for us to process their data so long as it does not impede our capacity to meet our legal obligations under relevant jurisdictional law.
- **Delete Personal Data**
  Individuals can ask us to erase or delete all, or some, of their Personal Data, so long as it does not impede our capacity to meet our legal obligations under relevant jurisdictional law.
- **Change or correct Personal Data**
  Individuals can ask us to correct some of their Personal Data, so long as it does not impede our capacity to meet our legal obligations under relevant jurisdictional law. They can also ask us to change, update or fix information about you in certain cases, particularly if it is inaccurate.
- **Object to, or limit or restrict use of Personal Data**
  Individuals can ask us to stop using all or some their Personal Data (for example, if we have no legal right to keep using it) or to limit our use of it (for example, if the information about them is inaccurate), so long as it does not impede our capacity to meet our legal obligations under relevant jurisdictional law.

- **Right to access Personal Data**
  Individuals can also ask us for a copy of their Personal Data in machine readable form if they reside in the EU, Australia or another country that provides this right as a matter of law.

Exercising these rights may be governed by an individual's contract with their employer, as it may impact on the provision of Seeing Machines' products and services and therefore driver safety.

Should an individual wish to exercise these rights in relation to Seeing Machines' products and services, they should contact their employer. Where relevant, they can write to us:

via e-mail at privacy@seeingmachines.com or

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

9. DATA PROTECTIONS

Personal Data is principally held in electronic databases maintained within the Seeing Machines Group's computer network. We maintain appropriate administrative, technical and physical safeguards designed to protect your Personal Data against accidental, unlawful or unauthorised destruction, loss, alteration, access, disclosure or use, consistent with this policy and relevant data protection legislation. We use the following mechanisms to protect Personal 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 legislation; and
- training and approvals – our 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.

10. COOKIES

We use cookies our across our websites to help enhance user experience, help make visits to our sites more effective and to collect industry-standard web statistics. Cookies are small data files which are sent from a web server to a web browser, and, depending on the type of cookie being used, either expire at the end of a browsing session or are stored until a set date.

Individuals can control the use of cookies at the individual browser level. Please note, however, that restricting the use of cookies may impact the functionality of our websites, particularly those that are designed to enable you to access a service. The three types of Cookies that we employ are:
1) essential (necessary to use the websites); 2) analytics (to help us understand how people use our websites); and 3) preference (to help us remember your language/ region choices).

We may provide links to other third-party websites which are outside of our control, individuals should review the privacy policies posted on the websites they visit.

11. NOTIFIABLE DATA BREACHES

We actively manage any suspected, actual or likely data breaches. We have put in place a data breach response plan and procedure as required by relevant legislation. Our employees must operate in accordance with these and our other data protection policies and procedures.

A data breach occurs when there is unauthorised access, transmission, copying, alteration, storage or disclosure of Personal Data or misuse of Personal Data. This may be as a result of malicious or criminal behaviour, system fault, human error or another factor.

We will notify affected individuals and relevant supervisory authorities, such as the Office of the Australian Information Commissioner, of a data breach, as required under relevant data protection legislation. Any notification of a data breach will be in accordance with the Australian Notifiable Data Breach Scheme and Articles 33 and 34 of the GDPR. These require reporting of any data breach that is likely to result in serious harm to or is likely to result in a high risk to rights and freedoms of an individual.

We may also have other obligations, outside of those contained in relevant data protection legislation, that relate to responding to certain types of data breaches, for example reporting obligations relating to “suspicious matters” under Australian *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

12. CROSS BORDER TRANSFERS

We primarily collect and process Personal Data in Australia and the United States. However, as we operate globally, Personal Data is collected in any country where we operate. It may therefore be stored and accessed in those countries. This Personal Data is collected and transferred pursuant to and in accordance with relevant data protection legislation (including, without limitation, the GDPR and any national laws implementing the GDPR). Transfer of Personal Data in most circumstances will be via a telecommunication or World Wide Web network.

Personal Data relating to products and services is normally stored within a database, which reside 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. When required by law, Seeing Machines may transfer Personal Data in accordance with the European Commission-approved Standard Contractual Clauses.

Some countries may not require the same level of protection for Personal Data as the country in which the Personal Data was collected. However, we maintain consistent data protection processes globally, similar to the requirements imposed under the GDPR, such as the safeguards afforded by the EU model clauses.

13. CONTACTING US

For further information about privacy, to lodge a complaint or exercise your Personal Data rights, please contact us:

via e-mail at privacy@seeingmachines.com or

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

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

14. UPDATES TO THIS POLICY

We reserve the right to change this policy from time to time. Any changes to this policy will become effective when we post the revised policy on our website.