SEEING MACHINES GROUP PRIVACY POLICY – EMPLOYEES, OFFICERS, DIRECTORS & APPLICANTS

1. INTRODUCTION

Seeing Machines Limited and its wholly-owned subsidiaries (the Seeing Machines Group) 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, applicable contracts, and our stakeholder's expectations.

2. SCOPE

This policy applies globally to all Personal Data of past, current and potential employees, officers and directors that is under the control of the Seeing Machines Group or our employees as a result of their work.

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 OF THIS POLICY

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 entities, 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. Entities 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. We are a "data controller" in relation to the Personal Data that we collect and process in relation to employees, officers, directors and applicants.

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 running our business, we collect Personal Data directly from employees, officers, directors and applicants, but may also collect Personal Data from other sources, such as an applicant's former employer/entity; an intermediary, such as a recruitment agency; or publicly available sources, such as LinkedIn or Facebook. The categories of Personal Data that may be collected is identified in table 1 below.

Table 1: Categories of Personal Data that May Be Collected

Categories of Personal Data	Applicants	Directors, Officers and Employees	Former Directors, Officers and Employees
Name and contact details.	√	√	√
Name of emergency contacts and their details.		√	√
Remuneration, such as current or former employment salary and/or equity information.	√	√	√
Copies of employment contracts, and other records relating to terms and conditions of employment.		√	√
Taxation and superannuation details.		√	√
Banking information necessary to pay salary and wages.		√	√
Records relating to salary, employment conditions, working hours, attendance and leave.		√	√
Records of travel and work-related expenses.		√	√
Information about educational and employment background.	√	√	√
Copies of academic qualifications.	√	√	√
Information about work eligibility, including nationality, country of residence, and visa and immigration status.	√	√	√

Categories of Personal Data	Applicants	Directors, Officers and Employees	Former Directors, Officers and Employees
Proof of Australian citizenship and/ work eligibility, such as copies of work visa.		√	√
CV and any attached supporting documentation to a resume.	√	√	√
Background check information, such as employment references or police checks.	√	√	√
Relevant information regarding health and/or disability to enable workplace adjustments.	√	√	√
Medical certificates (relating to an employee or a someone that they are caring for) or health related information supplied by an employee or their medical practitioner.		√	√
Other documents or certificates relating to leave (e.g. evidence relating to community service or a jury duty summons).		√	√
Information relating to employees' training and development.		√	√
Details of financial and other interests for the purpose of managing perceived or potential conflicts of interest or related matters.		√	√
Information about an employee's performance.		√	√
Photos for identification purposes.		√	√
System information, including user profiles, and information as to your interactions with those systems.		√	√

6. PURPOSE OF COLLECTION

We will only collect and use Personal Data for the purpose for which it was obtained. These purposes include, but are not limited to:

- managing recruitment processes and assessing applicants;
- engagement, transfer or promotion of employees, officers and directors;
- to perform our employer functions under law, such as meeting our workplace health and safety obligations;
- remuneration, payroll, taxation, and superannuation purposes;
- to administer and operate ICT systems and related policies and procedures;
- management of benefits, conditions, entitlements and related procedures;

- education, training and professional development;
- career development (including providing references), appraisals, succession planning, and performance management;
- the management of grievances and disciplinary procedures;
- business protection, including ensuring the security of our premises and systems, guarding against potential fraud or infringement of intellectual property, cyber-attack and other interference;
- to meet our governance obligations, as an entity trading on the Alternative Investment Market (AIM), a sub-market of the London Stock Exchange (LSE);
- operation of our business, such as disclosure of business contacts to our clients; and
- to assess compliance with regards to appointment or employment contracts, policies, and relevant legislation.

7. SHARING PERSONAL DATA

We may share Personal Data, as described in Table 1, with third parties:

- in order to fulfil our employer obligations, such as notifying relevant entities about commencement or cessation of an employee or payment of salary (e.g. the Australian Taxation Office or relevant superannuation entity);
- including our distributors and clients, to enable them to contact individuals, such as contact details for our sales staff;
- including our project partners, such as Monash University in relation to the Advanced Safe Truck Concept, to enable them to liaise with individuals about research or the provision of products and services;
- with written consent, to a new employer, for example if providing a reference;
- with written consent, to financial institutions, real estate agents and credit providers;
- with written consent, publicly or to a limited audience for marketing, promotion, tradeshow or media purposes, such as information about our executive which is published on our website;
- including contracted third-parties that collect or process Personal Data on our behalf, such as PeopleScout who provides our recruitment services;
- for scientific research to enhance, improve, or modify our products and services or to help develop new products and services;
- in order to meet our governance obligations as an entity trading on the AIM, such as notifications about services contracts with directors as required by Schedule 4 of the AIM Rules for Companies; and
- including 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 also share the Personal Data, as described in Table 1, 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 relevant 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.

8. RETENTION OF PERSONAL DATA

We retain the Personal Data, as described in Table 1, for a period of 7 years for the purposes outlined in this policy, unless a different retention period is required by jurisdictional law. If a person objects to us processing their Personal Data, we will remove it from our systems, unless we have a valid justification to hold on to it, such as to resolve a dispute or comply with our obligations under jurisdictional law.

9. PERSONAL DATA PROTECTIONS

Personal Data is principally held in electronic databases maintained within Seeing Machines' 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 our products or services or the operation of our business, 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 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.

10. CROSS BORDER TRANSFERS

We primarily collect and process the Personal Data, as described in Table 1, in Australia and the United States. However, as we operate globally, Personal Data may be 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).

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 and the Privacy Act.

11. PERSONAL DATA RIGHTS

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

- **Opt-out of our use of Personal Data**
  You may withdraw consent for us to process your data so long as it does not impede our capacity to meet our employer or legal obligations under relevant jurisdictional law.
- **Delete Personal Data**
  You can ask us to erase or delete all or some of your Personal Data, so long as it does not impede our capacity to meet our employer or legal obligations under relevant jurisdictional law.
- **Change or correct Personal Data**
  You can ask us to correct your Personal Data, so long as it does not impede our capacity to meet our employer or legal obligations under relevant jurisdictional law.
- **Object to, or limit or restrict use of Personal Data**
  You can ask us to stop using all or some your 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 you is inaccurate), so long as it does not impede our capacity to meet our employer or legal obligations under relevant jurisdictional law.
- **Right to access Personal Data**
  You can also ask us for a copy of your Personal Data in machine readable form if you reside in the EU, Australia or another country that provides this right as a matter of law.

Individuals may exercise these rights by writing 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

12. 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).

13. CONTACTING US

For further information about privacy, to lodge a complaint or exercise your Personal Data rights, 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 your 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.