PRIVACY POLICY

1. INTRODUCTION

(a) Redflex Holdings Limited ("**Redflex**") is an Australian public company listed on the Australian Securities Exchange whose registered office address is at 31 Market Street, South Melbourne, Victoria, Australia 3205. Redflex has subsidiaries in the United States of America (**U.S.**), Australia, United Kingdom (**U.K.**) and various other regions and countries (collectively, the "**Redflex Group**"). When we say "**Redflex**", "**we**" or "**us**" in this document, we mean Redflex Holdings Limited.

(b) This Privacy Policy (this "**Policy**") applies to information that Redflex and each entity within the Redflex Group. This Policy explains when and why we collect personal data about individuals, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

(c) Redflex is the data controller of personal data we collect. We are committed to respecting and protecting the privacy of individuals and entities, and we process personal data only in compliance with applicable data protection laws, including the Data Protection Regulation (EU) (2016/679) (the "**GDPR**"), the Data Protection Act 2017, any successor legislation to any of the above (together, the "**Data Protection Laws**").

(d) Redflex is also bound by the Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles set out in that act. We are also bound by other legislations (Australian Federal and its States and Territories) which may likewise require us to meet privacy obligations. Redflex will ensure it complies with the law in respect of privacy.

2. WHO IS COVERED BY THIS POLICY

(a) Failure to address privacy risk adequately and in compliance with the Data Protection Laws can cause reputational damage as well as increasing the risk of Redflex incurring legal penalties. The protection of personal data of donors, funders, event attendees and employees is fundamental to preserving trust between these individuals and Redflex.

(b) All directors, executives, employees, contractors and, by way of contract, commercial intermediaries who work for or are engaged by Redflex in any capacity and for any duration must comply with this Policy. Employees must observe this Policy. However, this Policy may be amended at any time and does not:

(i) form part of the terms of an employee's employment and it cannot be enforced by any employee as a contractual promise; or

(ii) give rise to any expectation of a particular outcome or decision on any matter arising under or pursuant to this Policy.

3. SCOPE OF THE POLICY

(a) All persons to whom this Policy applies are expected to comply with this Policy at all times.

(b) Breaches of this Policy by employees will be treated seriously and may lead to workplace disciplinary action up to and including termination of employment. For a non-executive director, if there is any breach of this Policy the non-executive may be asked to resign. For commercial intermediaries, if there is any breach of this Policy this may lead to the engagement being terminated.

4. RESPONSIBILITY FOR IMPLEMENTATION OF THE POLICY

(a) The Senior Vice President - Group General Counsel & Company Secretary has overall responsibility for ensuring Redflex' compliance with the Data Protection Laws and the effectiveness of this Policy. The Senior Vice President - Group General Counsel & Company Secretary is also responsible for monitoring and reviewing the operation of this Policy and making recommendations for changes to minimise risks to the operations of Redflex.

(b) All persons to whom this Policy applies are responsible ensuring Redflex's compliance with the Data Protection Laws and for their own compliance with this Policy and for ensuring that the Policy is consistently applied.

(c) All persons to whom this Policy applies should ensure that they take the time to read and understand this Policy.

(d) Any contraventions of this Policy should be reported to the Senior Vice President - Group General Counsel & Company Secretary, using the incident reporting function of RiCIR (Redflex' electronic Risk & Compliance and Incident Reporting tool) or via the whistle blower or ethics hotline.

(e) Questions regarding the content or application of this Policy should be directed to the Senior Vice President - Group General Counsel & Company Secretary.

5. DATA PROTECTION PRINCIPLES

Redflex' business operations shall at all times be consistent with the Data Protection Principles set out below. These principles are binding across our business.

(a) Lawful, fair and transparent processing

Our organisation only uses personal data in a way that is lawful, fair and transparent. We comply with data protection and privacy laws within each of the jurisdictions in which we operate. Where required by the law, we are also committed to helping individuals understand what information we collect, how we use it and what choices they have. We explain this to employees and business contacts in a simple and clear way in our privacy statements. We review our privacy statements regularly to keep them up to date, and to ensure they match our internal practices.

(b) Purpose limitation

We only collect personal data for specified, clear and legitimate purposes and we only collect as much personal data as we need to achieve those purposes. Though personal data helps us improve the services we provide, we only use it in ways which are proportionate to clear goals.

(c) Data accuracy

We take steps to ensure that the personal data we hold is accurate, up-to-date and relevant to the purposes for which it is collected.

(d) Data retention

We only keep personal data in an identifiable form for as long as is necessary for the purposes for which we are using it.

(e) Rights of the individuals

We are fully committed to address the privacy rights of individuals with respect to our processing of their personal data, in accordance with the applicable laws.

(f) Information security

We use appropriate technical and organisational measures to keep personal data secure and ensure its integrity, confidentiality and availability across all systems at all times. We are also committed to ensure that our vendors and suppliers which may process personal data on our behalf preserve the confidentiality, integrity and availability of such data.

(g) International transfers of personal data

Our organisation is a global business and as such we are required to transfer information internationally. We are fully committed to ensure that there are adequate safeguards in place, as required by the applicable laws, to protect the personal data we transfer to countries that do not have adequate data protection laws.

(h) Data protection accountability

We are all responsible for upholding the Data Protection Principles and respecting individuals' privacy rights. We have a collective and individual duty to protect our employees', business partners' and customers' personal data. In order to create an environment of trust and to comply with applicable data protection laws, all individuals operating within or on behalf of our organisation must comply with our privacy policies and help the organisation to uphold its commitments to the protection of personal data.

6. COLLECTION AND USE OF PERSONAL INFORMATION

(a) Kinds of personal information collected and held

(i) The types of personal information which Redflex processes include, an individual's name, contact details, bank account details, credit history and employment details (if applicable). In addition, Redflex processes special categories of personal data in relation to certain individuals, for example, details of criminal records or health information ("**Sensitive Personal Data**").

(ii) Exhaustive lists of the personal data that Redflex processes can be found in the Redflex Employee Privacy Notice and the Redflex Customer Privacy Notice.

(b) How personal information is collected

(i) Redflex collects and holds personal information on various individuals, including but not limited to its customers, suppliers, employees, contractors and commercial intermediaries. This information is collected in different ways including directly from employees, in meetings, by email, criminal background checks, medical checks, over the telephone and/or within written documentation including legal contracts.

(ii) Wherever possible, Redflex tries to only collect personal information directly from the individual. However, where Redflex requires personal information to be obtained from third parties or indirectly (for example independently verified criminal background checks), then Redflex will ensure that the relevant individual's consent is obtained to that sourcing and that the individual is aware of the purposes for which that information is to be collected, held and disclosed (as applicable).

(iii) Further information on the means by which Redflex collects personal data can be found in the Redflex Employee Privacy Notice and the Redflex Customer Privacy Notice.

(c) Purposes for which personal information is processed

(i) Redflex collects personal information for the primary purpose of normal business practices and operation, including to carry out its legal, regulatory, contractual and administrative obligations and requirements. In addition, Redflex may from time to time collect personal information for the secondary purpose of research and development, testing and provision of general data to regulatory bodies where it is required or requested to do so pursuant to legal, regulatory or contractual obligations.

(ii) Further information on the purposes for which Redflex processes personal data can be found in the Redflex Employee Privacy Notice and the Redflex Customer Privacy Notice.

(d) Marketing

Redflex does not actively engage in direct marketing activities to individuals. To the extent that Redflex decides to do so in the future it will only be done subject to consent given by individuals, who may at any time withdraw consent and request Redflex not to provide them with any direct marketing communications by contacting Redflex at the address below.

7. HOLDING OF PERSONAL INFORMATION

(a) Redflex predominantly holds personal information in an electronic format, although where required, it may transfer or receive the information into hard copy format. Redflex has specialised electronic systems, cloud software and encryption software

to protect the security of personal information and sensitive information. Access to such systems and software is only by authenticated and/or authorised users and groups.

(b) Where information is transferred into, or received in, hard copy, Redflex protects that information from unauthorised access, modification and/or disclosure by storing it in locked filing cabinets and only allowing approved persons with access to the required personal and sensitive information. Personal data is stored by us and/or our service providers and suppliers, strictly to the extent necessary for the performance of our obligations and strictly for the time necessary to achieve the purposes for which the information is collected, in accordance with the Data Protection Laws. When we no longer need to use personal data, we will remove it from our systems and records (either by shredding (hard copy) and/or securely destroyed with a certificate of guarantee (electronic copy)) and/or take steps to properly anonymise it so that the individual can no longer be identified from it (unless we need to keep that information to comply with legal or regulatory obligations to which we are subject).

(c) Some of the recipients we may share personal data and Sensitive Personal Data with may be located in countries outside of Europe. In some cases, this may include countries located outside the European Union and/or European Economic Area ("**EEA**").

(d) Some countries where recipients may be located already provide an adequate level of protection for this data and transfers to other countries such as the USA may be protected under arrangements such as the EU-U.S. Privacy Shield. Nonetheless, for transfers to Redflex entities outside of the EEA, Redflex will be bound by the EU Standard Contractual Clauses pursuant to Article 46(2)(c) GDPR, which the European Commission has assessed as providing an adequate level of protection for personal data, to ensure that personal data is protected adequately.

8. DISCLOSURE OF PERSONAL INFORMATION

In addition, Redflex will share certain personal information (including sensitive information) with third parties where required by Redflex to meet its legal obligations. Where Redflex shares personal information with unrelated third parties (unless an exception applies), Redflex will obtain the express consent of the relevant individual to the disclosure of personal information in this manner. In addition, Redflex uses a number of service providers contractors and commercial intermediaries to whom it discloses personal information. Redflex enters into written contracts to protect this personal information, including requirements for the third party to use or disclose information only for the purposes of the contract and additional special privacy requirements where necessary.

9. PRIVACY PROGRAMME

The Senior Vice President - Group General Counsel & Company Secretary will supervise the Privacy Programme, which provides a comprehensive, coordinated approach to managing privacy risk while serving business needs and strategies. The Privacy Programme comprises, at a minimum, the following components:

(a) Policy framework

Our organisation shall operate at all times in compliance with this Policy, the Employee Code of Conduct and Ethics and all internal policies, procedures and standards relating to privacy and privacy notices to staff, customers and other individuals. Please note that these may, from time to time, be updated or replaced and the scope of the list below may be expanded to additional policies.

(b) Legal compliance

The Senior Vice President - Group General Counsel & Company Secretary will at all times maintain processes that enable our organisation to understand and comply with legal requirements in data protection such as providing privacy notices to data subjects and obtaining their consent to data processing where necessary. The Senior Vice President - Group General Counsel & Company Secretary will ensure that privacy laws are addressed consistently across the region where such laws apply.

(c) Documentation of data protection compliance (decisions, implementation and audit)

(i) The Senior Vice President - Group General Counsel & Company Secretary, supported by the business functions concerned, will create and maintain records of the decisions and actions taken towards privacy risk management and compliance with data protection laws. This will also enable effective collaboration with the regulators as and when required and it will enable our organisation to document and demonstrate its privacy compliance at all times.

(ii) Where privacy related decisions and actions are taken at regional or business level, the relevant policies and procedures will establish ownership of and responsibility for maintaining appropriate records.

(iii) The Senior Vice President - Group General Counsel & Company Secretary will also be responsible for ensuring and supervising the development of any additional records which may be required to demonstrate compliance under applicable data protection laws (e.g. consent forms, notices to data subjects, register of personal data breaches).

(d) Records of processing activities

The Senior Vice President - Group General Counsel & Company Secretary will gather in a living document the list of all processing activities within Redflex at a given time. This document will be updated from time to time to reflect changes in business operations. The IT and People & Performance Teams and any other business functions involved in the processing of personal data should contribute to the record of processing activities (providing relevant information such as about the purposes of use of data and data transfers).

(e) Data protection impact assessments ("DPIAs")

The Senior Vice President - Group General Counsel & Company Secretary will establish guidelines and procedures to perform DPIAs with respect to new products,

technologies and business operations, where required by applicable laws or where this appears appropriate to manage privacy risk. The DPIAs will require the input and involvement of the relevant business functions.

(f) Vendor privacy risk management

Risk management for engaging third party vendors that process personal data on behalf of Redflex ("data processors") is crucial to ensure Redflex' data protection compliance. The Senior Vice President - Group General Counsel & Company Secretary will provide guidelines and any privacy content necessary for third party risk assessment, keeping it up-to-date as necessary to address emerging privacy risks. Risks associated with a third party must be escalated to the Senior Vice President - Group General Counsel & Company Secretary.

In particular, the Senior Vice President - Group General Counsel & Company Secretary will ensure that:

(i) any data processor is subject to adequate due diligence on its information security measures before being selected by Redflex as a business partner;

(ii) an appropriate processing agreement is in place with any data processor which imposes data protection obligations on the data processor; and

(iii) data processors' compliance with the processing agreement and the applicable law is monitored from time to time.

(g) Data protection training

Data protection training will be a part of the annual compliance training plan and required to all employees upon joining the firm and on a regular basis. The Senior Vice President - Group General Counsel & Company Secretary will ensure that training content remains up to date and appropriate to our organisation’s business operations, and that it is refreshed on a regular basis. Training completion rates will be monitored and documented (e.g. training log).

(h) Data breach management

(i) All business functions are responsible for monitoring business operations for incidents concerning the security of personal data, capturing them on a timely and consistent basis, and executing appropriate risk mitigation strategies.

(ii) All employees and business functions are responsible for immediately escalating any actual or suspected data breaches according to our [Data Breach Management Policy.] Any relevant office and business function is required to take part in breach management according to such policy.

(iii) The Senior Vice President - Group General Counsel & Company Secretary will ensure that known incidents and risk events are identified, evaluated and remediated appropriately, and will evaluate trends so that root causes can be addressed. The Senior Vice President - Group General Counsel &

Company Secretary will also handle breach notifications to the competent regulator or data subjects as and when required by the applicable laws.

(i) Data subject rights

The Senior Vice President - Group General Counsel & Company Secretary will provide guidelines and assistance to business functions to address any data subject right request (e.g., an individual's request to access personal data held by Redflex) in accordance with the applicable law.

10. WHAT EMPLOYEES MUST DO

(a) Apply the Data Protection Principles to the collection and use of personal data and follow the policies, procedures and standards regarding privacy:

(i) Learn how to identify personal data and report any queries to the Senior Vice President - Group General Counsel & Company Secretary care of Redflex Holdings Limited, 31 Market Street, South Melbourne, Victoria 3205, Australia, telephone +61 3 9093 3324 email redflexholdingslimited@redflex.com.au.

(ii) Only collect personal data that is directly relevant and necessary to accomplish the specified purpose(s) and only retain personal data for as long as is necessary to fulfil the specified purpose(s) (as set out in the Employee Privacy Notice or the Customer Privacy Notice, as applicable).

(iii) Use personal data solely for the purpose(s) for which it was collected (as set out in the Employee Privacy Notice or the Customer Privacy Notice, as applicable).

(iv) Ensure that personal data is accurate, up-to-date and relevant to the purpose(s) for which it is collected (as set out in the Employee Privacy Notice or the Customer Privacy Notice, as applicable).

(v) Secure personal data (paper and electronic) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure (e.g. avoid leaving papers, documents or files containing personal data in plain view when you are away from your work area).

(vi) Avoid accessing, collecting or storing personal data that is not necessary for their current job responsibilities.

(vii) Always dispose of personal data securely, for example by shredding or appropriate electronic erasure.

(viii) Remember that personal data belongs to Redflex and may not be copied, transferred or otherwise removed without permission.

(b) Use Redflex data and equipment appropriately

(i) Use Redflex data and equipment for legitimate business purposes only and in accordance with applicable policies, guidelines and instructions.

(ii) Do not install or use any other software on their computer without Redflex's approval.

(iii) Manage business applications on Redflex computers and telecommunications devices in accordance with Redflex's Information Security Policy.

(c) Report data breaches

Immediately report the following situations to the Senior Vice President - Group General Counsel & Company Secretary:

(i) any suspicious activity related to a computer, network, or software application;

(ii) any potential or actual loss, misuse, improper access or modification of personal data (including loss of electronic mobile devices or paper records);

(iii) the security of any system or device containing personal data has been compromised;

(iv) that personal data has been accessed, used or disclosed in violation of any applicable policy; or

(v) any other actual or suspected data breach.

Once submitted, the incident will be investigated and corrective actions implemented, as necessary.

(d) Complete required training

Undertake and complete all required data protection training.

(e) Consequences in case of non-compliance

Non-compliance with the terms of this Policy may result in disciplinary action up to and including termination of employment or business relationship, as well as legal action.

11. NOTIFIABLE DATA BREACHES

(a) A notifiable data breach occurs when personal information held by Redflex is lost or subjected to unauthorised access, disclosure or other misuse or interference that is likely to result in serious harm to any individual. Serious harm can include psychological, emotional, physical, reputational or other harm.

(b) In addition to the matters in paragraph 10(c) of this Policy, if any employee suspects a data breach has occurred please refer to the Data Breach Response Plan, report it to the Senior Vice President - Group General Counsel & Company Secretary or follow the complaints procedure below.

12. REVIEW OF POLICY

(a) Redflex will review this Policy periodically (and no less that once per year) to ensure it complies with applicable legal requirements and remains relevant and effective.

(b) This Policy is not intended to be contractual in nature.

(c) Redflex may change this Policy at any time.

13. EXCEPTIONS AND ESCALATIONS

(a) Any exception to this Policy must be reviewed and approved by the Senior Vice President - Group General Counsel & Company Secretary. All exceptions to this Policy must be approved before implementation.

(b) The Senior Vice President - Group General Counsel & Company Secretary is responsible for resolving questions about the appropriate interpretation of this Policy in light of legal and regulatory requirements. The Senior Vice President - Group General Counsel & Company Secretary is responsible for addressing questions about interpreting this Policy.

CHANGE HISTORY

Version	Description	Date
1.0	Initial Version	22 July 2016
2.0	Annual Review	24 May 2017
3.0	Annual Review	19 March 2018
4.0	GDPR Compliance Review	25 May 2018