AGREEMENT FOR THE SAFEGUARD OF ELECTOR INFORMATION

VEDA ADVANTAGE INFORMATION SERVICES AND SOLUTIONS LTD NOW KNOWN AS EQUIFAX AUSTRALIA INFORMATION SERVICES AND SOLUTIONS PTY LIMITED ABN 26 000 602 862

I, [redacted], Group Managing Director, Australia and New Zealand, make this Deed Poll on behalf of the Veda Advantage Information Services and Solutions Ltd, now known as Equifax Australia Information Services and Solutions Pty Limited (**'the Organisation'**), a prescribed organisation specified in the table at subsection 8(1) of the *Electoral and Referendum Regulation 2016* (**'the Regulation'**), understand and agree that the Australian Electoral Commission (**'AEC'**) may give a copy of a Roll (or an extract of a Roll) (**'Elector Information'**) to the Organisation under items 5 and/or 7 of the table in subsection 90B(4) of the *Commonwealth Electoral Act 1918* (Cth) (**'the Electoral Act'**) subject to compliance with this Agreement for the Safeguard of Elector Information ('**the Safeguard Agreement**').

1. Provision of Elector Information

1.1. For the purpose of the Safeguard Agreement the Elector Information that may be provided to the Organisation, on request by the Organisation and payment of the fee in accordance with clause 10, is:

(a) Surname and given names; and

(b) Real place of living (Note: Address information cannot be provided in relation to silent electors and is not available for itinerant and eligible overseas electors).

1.2. Notwithstanding this Safeguard Agreement, the Electoral Commission or delegate may exercise its discretion to not give the Organisation Elector Information at any time.

2. Use of Elector Information

2.1. The Organisation must ensure that Elector Information is not used for any purpose other than the permitted purpose as specified in section 91A of the Electoral Act.

2.2. The permitted purposes under items 5 and 7 of the Electoral Act for the Organisation are:

(a) to verify, or contribute to the verification of, the identity of persons for the purposes of the *Financial Transaction Reports Act 1988* (**'FTR Act'**);

(b) to facilitate the carrying out of applicable customer identification procedures under the AML/CTF Act.

2.3. The Organisation must ensure that Elector Information:

(a) is stored and communicated securely in accordance with clause 3 below;

(b) is not accessed by any:

(i) person (other than as permitted under clause 4); or

(ii) organisation that is not the relevant Organisation prescribed in column 3 of the table in Part 2, subsection 8(1) of the Regulation in respect of the Organisation;

(c) that persons permitted to access the Elector Information are aware of the conditions and penalties specified in clause 4.5 below; and

(d) is destroyed and deleted in accordance with clause 5 below.

2.4. The Organisation will ensure that the end user of the identity verification check is notified that the source of the Elector Information used to enable the check is the AEC.

3. Data security, confidentiality and protection of Elector Information

3.1. The Organisation acknowledges that it is an 'APP entity' as defined by the *Privacy Act 1988* (Cth) (**'the Privacy Act'**) and as such will, at all times, comply with the requirements of that Act.

3.2. The Organisation acknowledges that Elector Information received under items 5 and/or 7 of the table in subsection 90B(4) of the Electoral Act includes confidential and personal information and agrees to:

(a) take all reasonable steps to ensure that the Elector Information supplied is protected against loss, and against unauthorised access, use, modification, disclosure or other misuse;

(b) not disseminate any publications or information otherwise released from data compilations in a manner that is likely to enable the identification of a particular person;

(c) ensure that access to Elector Information is in accordance with clause 4 of this Safeguard Agreement; and

(d) ensure that all Elector Information is stored within a system with adequate controls on access in accordance with clause 3.7 of this Safeguard Agreement.

3.3. The Organisation must notify the AEC of all unauthorised access, use, modification or disclosure of Elector Information irrespective of whether a report is made to the Office of the Australian Information Commissioner (**'OAIC'**). This notice must be in writing, and provided as soon as the Organisation is aware of the unauthorised use or disclosure.

3.4. In accordance with the mandatory Notifiable Data Breach (**'NDB'**) scheme under Part IIIC of the Privacy Act, if the Organisation becomes aware, or has reasonable grounds to suspect, a data breach has occurred, involving Elector Information that is personal information that is likely to result in serious harm to any individual affected the Organisation must:

(a) undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected; and

(b) notify the AEC of any Eligible Data Breach (as that term is defined in the Privacy Act), in writing as soon as practicable; and

(c) if the assessment determines that the breach constitutes an eligible data breach, notify the OAIC; and

(d) notify all affected individuals in accordance with the NDB Scheme.

3.5. When reporting an Eligible Data Breach, the Organisation will provide the AEC with full details of the reported breach and copies of any reports or communications between the organisation and the OAIC relevant to the reported data breach.

3.6. If the Organisation receives a complaint alleging interference with the privacy of an individual by the Organisation arising out of operations within the permitted purpose for the use of the Elector Information the Organisation will:

(a) immediately notify the AEC of the nature of that complaint and such details of that complaint as are necessary to minimise any (or further) interference; and

(b) keep the AEC informed as to the progress of that complaint as it relates to the Organisation's actions in connection with that allegation of interference.

Storage of Elector Information

3.7. The Elector Information must be stored and communicated securely and the Organisation must ensure that the Elector Information:

(a) is not copied (except when uploading the Elector Information in accordance with sub-clause 2.3 or as part of standard system redundancy and backup process);

(b) is uploaded to a computer facility that is owned and operated solely by the Organisation or is operated and maintained by a third-party under contract with the Organisation. Any terms of the relevant contract must mirror section 95B of the Privacy Act;

(c) is stored on a computer facility in such a way as to restrict access to the Elector Information, including any standard system redundancy and backup copies, to permitted persons in accordance with clause 3; and

(d) where there is a need to communicate the Elector Information for use in accordance with this Safeguard Agreement, the Elector Information must be encrypted using a Commonwealth Government approved protocol.

3.8. The Organisation must not transmit, hold or process the Elector Information outside Australia.

3.9. The Organisation must disclose in writing to the AEC all third-party vendors that have access to their IT systems and notify the AEC within one month of any contractual change of third-party vendor.

3.10. The Organisation must disclose in writing to the AEC any system that stores Elector Information which is managed by a third-party vendor.

3.11. Clause 3 will survive the expiration or termination of this Safeguard Agreement.

4. Access to Elector Information

4.1. The Elector Information must only be accessed and used for a permitted purpose by:

(a) the Organisation's employees, who work in a team that has been authorised by the Group Managing Director to access Elector Information based on a genuine need for the performance of duties; or

(b) those persons who provide services to the Organisation under a contract (**'Contract Staff'**) who have executed a Deed Poll under sub-clause 4.2, who work in a team that has been authorised by the Organisation to access Elector Information based on a genuine need for the performance of duties. This definition of Contract Staff includes staff at a third-party vendor that manages any system which stores Elector Information.

4.2. The Organisation must require all of the Organisation's employees and Contract Staff, who may access, use or disclose Elector Information as part of their employment duties, to execute a Deed Poll provided by the AEC as to the Permitted Purpose of Elector Information before accessing the Elector Information as part of their duties. The Organisation must inform the AEC if an Organisation employee and/or Contract Staff member who has executed a Deed Poll is no longer accessing, using or disclosing Elector Information.

4.3. The Organisation must require all of the Organisation's employees and Contract Staff, who may access, use or disclose Elector Information as part of their employment duties to undertake training which outlines the sensitivity of the data and their legislative requirements as referenced in this Safeguard Agreement.

4.4. The Organisation must capture and log all records of training attendance, including the dates that the training was undertaken.

4.5. The Organisation must ensure that its employees and Contract Staff are made aware that:

(a) the use of Elector Information for purposes other than a permitted purpose may constitute a breach of section 91A of the Electoral Act, which carries a penalty of up to 100 penalty units. The value of a penalty unit is set by section 4AA of the *Crimes Act 1914* (Cth) and is currently $210);

(b) an offence under Division 478 of the *Criminal Code Act 1995* (Cth) (**'the Criminal Code'**) may be committed by:

(i) unauthorised access to, or modification of Elector Information for a purpose that is not a permitted purpose. If a person is found guilty of an offence under 478.1 of the Criminal Code, a court may impose a maximum penalty of up to 2 years imprisonment;

(ii) unauthorised impairment of the reliability, security or operation of the data held on the disk or other medium containing the Elector Information. If a person is found guilty of an offence under 478.2 of the Criminal Code, a court may impose maximum penalty of up to 2 years imprisonment;

(iii) possession or control of Elector Information with intent to commit a computer offence. If a person is found guilty of an offence under 478.3 of the Criminal Code, a court may impose maximum penalty of up to 3 years imprisonment; or

(iv) producing, supplying or obtaining the Elector Information with the intent to commit a computer offence. If a person found guilty of an offence under 478.4 of the Criminal Code, a court may impose maximum penalty of up to 3 years imprisonment.

(c) the Elector Information must remain in the Organisation's power, possession or control and must be securely stored at all times.

4.6. The Organisation must undertake an annual review of user access rights to ensure user access rights to the data are commensurate with roles and responsibilities.

4.7. The Organisation must log all access to and undertake the monitoring of audit logs, to monitor for the ongoing appropriate use/access to the Elector Information.

4.8. The Organisation must retain the inputs (e.g. user listings or audit logs that were reviewed) and outputs (e.g. actions undertaken after the review) of both forms of review outlined above and provide these inputs and outputs to the AEC where required and upon request by the AEC.

5. Destruction of Elector Information

5.1. On the earlier of:

(a) the expiration of the period ending six months after the receipt of the Elector Information by the Organisation, or

(b) the receipt of an updated version of the Electoral Information (or earlier if the Organisation decides that it no longer requires the Elector Information).

The Organisation must ensure that any medium containing the Elector Information provided by the AEC, including all copies of the Elector Information (as distinct from information about an individual that is merged in the Organisation's records for the relevant permitted purpose) is:

(c) securely deleted and destroyed in accordance with the destruction instructions provided by the AEC; or

(d) delivered to the AEC by registered mail.

5.2. Within two weeks of the occurrence of an event specified in clause 5.1, and at the direction of the AEC, the Organisation must provide to the AEC a Certificate of Destruction (using the template provided) that attests to the:

(a) deletion of the Elector Information earlier uploaded to the computer facility; and

(b) destruction or return by registered mail of the discs or other medium provided by the AEC that contain the Elector Information provided before the receipt of the new Elector Information from the AEC (as the case requires).

5.3. The Organisation acknowledges that the provision of Elector Information remains at the discretion of the AEC and any request for access to such information by the Organisation may be refused. The Organisation may not be provided the next provision of Elector Information if the AEC is not satisfied that destruction has occurred.

6. Security Incidents

6.1. For the purposes of this agreement a **'Security Incident'** is any event that indicates that the security of an information system, service or network has been, or may have been, compromised.

6.2. The Organisation must immediately advise the AEC's National Enrolment Services Section (via email to rps@aec.gov.au) of any Security Incident involving Elector Information.

7. Organisational Change

7.1. The Organisation will advise the AEC of any proposed changes to organisational structure or business process that may impact on the way Elector Information is accessed or used. This includes, but is not limited to, any new contractual arrangements which may facilitate a wider use of the Elector Information for the FTR Act and/or AML/CTF Act purposes.

8. Annual Assurance

8.1. The Organisation must provide the AEC with an annual statement of assurance before 30 June each year that the Elector Information has been used in accordance with the Safeguard Agreement.

8.2. Where the Organisation fails to provide such assurance, no further Elector Information will be provided until the AEC is fully satisfied that the Organisation is operating in strict conformance with the Safeguard Agreement.

9. Audits of the Management of the Elector Information

9.1. The Organisation must undertake an independent audit of its compliance with the provisions of this Safeguard Agreement every three years. The audit must be undertaken at the expense of the Organisation and be undertaken by an auditor approved by the AEC Information Technology Security Advisor and the Assistant Commissioner responsible for Assurance at the AEC.

9.2. The audit must be prepared pursuant to the provisions of the Standard on Assurance Engagements (ASAE 3150) issued by the Auditing and Assurance Standards Board.

9.3. The Organisation must provide a copy of the audit report to the AEC within one (1) month of the audit report being available.

9.4. If an issue identified in an audit report has not been addressed to the AEC's satisfaction within 30 business days after receipt of the audit report, the Electoral Commission or delegate may exercise its discretion to not give the Organisation Elector Information. The AEC may also direct the Organisation to destroy Elector information that it holds in accordance with clause 5, where an audit report identifies non-compliance with the Safeguard Agreement.

9.5. The Organisation must report to the AEC, the results of internal and external audit/assurance activities undertaken in relation to systems and processes, as relevant to the management of the Elector Information. This includes independent assurances that third-party vendors are subject to, such as ISO-37000 compliance audits, to ensure their IT systems are secure.

9.6. The AEC may, on no less than ten (10) working days' notice, undertake inspections and/or audits of the Organisation no more than once a year, at the Organisation's cost to check the Organisation's compliance with its requirements outlined in this Safeguard Agreement, or any Certificate of Destruction or Deed Poll signed by or required to be signed by the Organisation. The Organisation agrees to provide the AEC or its agents with reasonable access to their sites to facilitate inspections and/or audits.

10. Financial arrangements

10.1. The Organisation understands that the AEC is entitled to recoup the costs incurred by the AEC in providing Elector Information to the Organisation in accordance with subsection 90B(9) of the Electoral Act.

10.2. The Organisation must pay the service fee and receipt of the payment must be confirmed in order for the AEC to provide Elector Information.

11. Review and termination of the agreement

11.1. This Safeguard Agreement will commence upon execution and expire three years from the date of execution.

11.2. The AEC may at any time review and vary the terms and conditions of this Safeguard Agreement and require the execution of a new Safeguard Agreement.

11.3. The AEC may at any time by written notice, terminate this Safeguard Agreement.

11.4. Upon receipt of a notice of termination from the AEC, the Organisation must:

(a) securely destroy or deliver to the AEC the Elector Information which is in the Organisation's power, possession or control; and

(b) provide the AEC with a statutory declaration confirming that the secure destruction of the Elector Information or the secure delivery of the Elector Information to the AEC is complete and in accordance with this clause.

11.5. [redacted]

11.6. Any notice under this Safeguard Agreement is only effective if it is in writing, signed by the person giving the notice and either delivered by hand, sent by pre-paid post, or transmitted electronically by electronic mail.

11.7. A notice:

(a) must be sent to the Relevant Address using one of the means specified in the following subparagraphs:

(i) by hand or courier;

(ii) by post; or

(iii) electronic transmission; and

(b) subject to paragraph (c) is delivered on a business day if delivery occurs before 5 p.m. or otherwise on the next business day; and

(c) is taken to have been delivered on a business day:

(i) by post, on the date that it should arrive in the ordinary course of the post from the date of posting for the method of postage used by the person giving the notice;

(ii) by electronic transmission on the day and at the hour of transmission, unless the sender receives a notice of failure of the transmission.

11.8. For the purposes of clause 11.7 the Relevant Address is for a notice to:

(a) the AEC to be directed to the attention of the National Enrolment Services Section at:

(i) street address:

50 Marcus Clarke Street

Canberra ACT 2600

(ii) postal address:

Locked Bag 4007

Canberra ACT 2601

(iii) email: rps@aec.gov.au

until otherwise notified by the AEC to the Organisation;

(b) the Organisation to be directed to the attention of [state] at:

(i) street address: Level 15, 100 Arthur Street, North Sydney NSW 2060

(ii) postal address: Level 15, 100 Arthur Street, North Sydney NSW 2060

(iii) email**:** companysecretariat@equifax.com

Until otherwise notified by the Organisation to the AEC.

12. Execution

Executed as a Deed on 6th April 2020

Signed by Lisa Marie Nelson, Group Managing Director, Australia and New Zealand who is duly authorised to make this Deed on behalf of the Organisation in the presence of:	))))))))))

Lisa M. Nelson

(Signature)

(Signature of witness)

Monica Pasca

.....

(Name of witness)