Equifax Australasia Workforce Solutions Pty Ltd

ABN 86 080 799 720

SOW for fit2work® (Australia & New Zealand)

Effective 28th November 2024

1. Introduction

1.1 This statement of work ("**SOW**") applies when we, Equifax Australasia Workforce Solutions Pty Limited ABN 86 080 799 720 ("**Equifax**") supply any fit2work® product services ("**fit2work**") to you, our customer, under our terms of supply for information services accessible electronically at *www.equifax.com.au/hrsolutions/pdf/terms-of-supply.pdf* ("**Terms of Supply**"). Those Terms of Supply and this SOW govern our provision of the fit2work services to you. Additional terms may also apply to various types of fit2work services we supply; if so, those additional terms are set out in a Subscription Agreement, an Onboarding Form, Work Order, Fee Schedule or other collateral document (such as a schedule, exhibit or appendix) executed by you and us for purposes of the relevant information service.

1.2 Where other specific contractual arrangements have been executed and are in place between you and us, this SOW applies only to the extent not inconsistent with those contractual arrangements.

1.3 Where this SOW uses terms defined by the Terms of Supply that it does not separately define in Schedule 1 to this SOW, those terms have the same meaning in this SOW unless the context otherwise requires. The terms defined in Schedule 1 to this SOW have the same meaning where used in this SOW, unless the context otherwise requires.

1.4 fit2work services are provided in accordance with its Collection Statement accessible at *www.equifax.com.au/hrsolutions/pdf/fit2work-collection-statement.pdf.*

1.5 Our fit2work services comprise both automated or manual methods of providing income and employment verifications in respect of an Applicant nominated by you and include:

A. National and worldwide identity verification searches;
B. Australian police and criminal background checks through AFP and ACIC;
C. NZ criminal conviction checks through the Ministry of Justice;
D. Other international criminal history and identity checks;
E. Professional history qualification & registration checks;
F. ANZ licensing checks (including ASIC, APRA and directorship records);
G. Employment history and behavioural reference checks;
H. At the direction of the Applicant, financial history and credit checks accessed through our Affiliate using its independent consumer and commercial credit reporting services;
I. Medical checks through various health service providers;
J. Information in relation to COVID-19 vaccination status including collection of evidence of vaccination status (including vaccination certificates) provided by the Australian or New Zealand Government;
K. Interface with HR platform management systems for workforce management across the employment cycle;
L. Various other related workforce data search services; and
M. Consolidated reporting

.

1.6 Where you are a Consumer, you may have access to a limited number of our fit2work services (including, for example, searches offered by ACIC, the AFP or the MoJ, or purchasing a fit2work Badge). If you are a Consumer, clauses 2 and 5 (other than clause 5.1(e)) of this SOW apply to you. For the avoidance of doubt, where you are a business that is treated as a Consumer, the balance of the provisions in this SOW also apply to you to the extent not inconsistent with clause 2 of this SOW.

2. Supply of fit2work services – Consumer

2.1 When purchased by a Consumer, the fit2work services come with consumer guarantees that cannot be excluded under the relevant Consumer Law. In such a case, subject to the relevant Consumer Law and as contemplated by clause 10 of the Terms of Supply, if a guarantee is not satisfied you may be entitled to a resupply of that service or payment of the cost of having that service supplied again, as well as to cancel the service.

2.2 Nothing in this SOW is intended to exclude, restrict or modify any rights that you may have under the relevant Consumer Law or any other applicable legislation which may not be excluded, restricted or modified by agreement.

2.3 For the purposes of section 5D of the FTA (NZ) and section 43 of the CGA (NZ), to the extent permitted by Law, where you are a business (including as a sole trader):

(a) the fit2work services provided to you under or in connection with this SOW are being provided and acquired in trade;
(b) if either or both the FTA (NZ) or the CGA (NZ) applies to the supply of the fit2work services to you then, in respect of all matters under or in connection with this SOW, the parties are contracting out of the CGA (NZ) and sections 9, 12A and 13 of the FTA (NZ); and
(c) it is fair and reasonable for the parties to be bound by this clause 2.3.

2.4 Where you apply for any fit2work service as an Applicant at the request (or otherwise knowingly for the benefit) of an employer who is also our customer, you acknowledge that:

(a) we act as the agent of that employer as contemplated by clause 2.2 of the Terms of Supply; and
(b) to the extent that we may also otherwise act, or be seen as acting, as your agent for purposes of performing an information service (including obtaining search results or providing a report to that employer), you:

(i) have full knowledge of our role as agent of the employer;
(ii) have read and understood the Collection Statement accessible at www.equifax.com.au/hrsolutions/pdf/fit2work-collection-statement.pdf;
(iii) are aware of any material facts which might affect you in any dealings with your personal information by us as agent for the employer (for example, if you are a bank employee, disclosure of potential departure to a current employer, through compliance with the *ABA Conduct Background Check Protocol*);
(iv) freely consent to our involvement for the employer and any transactions contemplated by this SOW for its benefit; and
(v) waive any conflict of interest or fiduciary duty otherwise owed to you to the extent inconsistent with that consent.

2.5 Where, as Applicant, you are resident in the EU at the time we process personal information as part of our information services, we act as a data controller or joint data controller and a data importer. In those circumstances, we comply with our GDPR obligations in respect of your personal data as set out in schedule 4 to our Collection Statement. A supplier of data to us for purposes of those services may function as a data processor under the GDPR, in accordance with that supplier's service contract with us.

2.6 Where, as Applicant, you are under 18 years of age, a parent or guardian may complete an application for a fit2work service on your behalf and that person will be taken to have certified that the personal information provided by them regarding you is true, correct and not misleading in any material particular. You acknowledge that your participation, whether directly or through the act of a parent or guardian, in applying for a fit2work service is a civil act which is for the benefit of you as a minor participant and is fair and reasonable as at the time you apply for the services.

2.7 (a) Where, as an Applicant, you purchase a fit2work Badge, you purchase a:

(i) 'Gold fit2work Badge' (including police, entitlement to work (visa) and primary qualifications checks);
(ii) 'Silver fit2work Badge' (including police and entitlement to work (visa) checks); or
(iii) 'Bronze fit2work Badge' (including police check only), (each a 'fit2work Badge', as defined in Schedule 1 below).

(b) All fit2work Badges include an ACIC police check and the badge will expire 3 months from the date of purchase, unless your subscription is maintained.
(c) If your police check is clear and once all your applicable fit2work Badge check results have been provided to you, you may share your fit2work Badge securely with an employer.
(d) We make no warranty or guarantee that a fit2work Badge will be accepted by an employer or that your fit2work Badge is sufficient to meet an employer's background screening requirements, policies or processes.

3. Supply of fit2work services – B2B

3.1 Consistent with clause 4.8 of the Terms of Supply, you will appoint a representative who is to be responsible for the business relationship with us for our fit2work services and who is to be the single point of contact for us and, as may be relevant, the AFP and ACIC. In the absence of any notice from you specifying an Authorised Officer, the officer executing your Onboarding Form or otherwise deemed as accepting this agreement (or any successor in that position from time to time) will be your Authorised Officer.

3.2 The Authorised Officer is authorised to accept notices on your behalf in respect of fit2work services and is responsible for:
(a) contract management and compliance;
(b) your performance as that relates to our provision of fit2work services; and
(c) supporting us in developing the capability to provide the reports contemplated by this SOW.

3.3 We will undertake the checks that you request and report on those in the fastest time practicable. We are not liable for any delay or failure to provide information arising from, or caused or contributed to by, your acts or omissions or those of any third party; however, we will employ all reasonable endeavours to complete the checks and will notify you in a timely manner if this cannot be done.

3.4 You and your Personnel must provide us with all information, materials, assistance and decisions required to enable us to provide the fit2work services and otherwise perform our obligations under this SOW. In particular, you acknowledge that we cannot action any check request until we receive the necessary informed consent from the Applicant.

3.5 We will make a maximum of three attempts to verify information or obtain missing information in respect of a check before closing that verification or search as "unverified". Our fit2work service is then complete upon reporting to you that the verification or search is "unverified".

3.6 If we request you, or the Applicant, to provide further instructions and we do not receive any adequate response to that request, we reserve the right to close any related search; however, we will not close any such search before the date that is 14 days after we make that request for further instructions.

3.7 You acknowledge that we:
(a) obtain all data supplied as part of the fit2work services from third parties and rely on those suppliers of data to take reasonable steps to ensure that the data provided is accurate; and
(b) do not independently verify the data that we obtain and supply and do not provide any guarantee or

warranty as to the accuracy or completeness of any such data provided to you or an Applicant.

4. Your use of our information services

4.1 You must use the fit2work services, and any information provided to you as a part of those services, for the Approved Purpose only and at all times comply with our agreement (including this SOW) and all applicable Laws in all jurisdictions that relate to your access to and use of those services.

4.2 Without limiting clause 4.1 of this SOW, you must:
(a) in dealing with any personal information, comply with all Privacy Legislation by which you are or have agreed to be bound;
(b) restrict access to any personal information to Personnel who need to access that personal information to fulfil your obligations for the Approved Purpose;
(c) not disclose or permit the disclosure of personal information to any third party including, without limitation, a third party outside the jurisdiction in which the information is initially received by you, unless:
(i) expressly required or permitted under this agreement; or
(ii) otherwise with our prior written consent, which may be conditional;
(d) take all reasonable steps to ensure that the personal information is protected against misuse and loss, or unauthorised dealing, including by:
(i) undertaking any staff training as may be required;
(ii) monitoring staff and third-party use of any personal information;
(iii) procuring compliance with clause 3 of this SOW by any third party or Personnel to which you have disclosed or permitted disclosure of any personal information;
(e) take such steps we reasonably require of you to facilitate our compliance with the Privacy Legislation, including cooperating with us to resolve any complaint alleging a breach of any Privacy Legislation in respect of any actual or alleged dealing with personal information by you or any of your Personnel (as contemplated by clause 10.8 of the Terms of Supply);
(f) not do or omit to do any act that would put us in breach of any Privacy Legislation; and
(g) immediately notify us if you become aware of a breach of the Privacy Legislation in connection with this agreement.

4.3 Without limiting clause 3.4 of this SOW, you acknowledge and agree that where, to provide the fit2work services, we need to transfer personal information of an Applicant to a third party, you have (or will obtain within the requisite timeframe) a valid authority of that Applicant to allow us to make that transfer.

4.4 Where you place an order for the provision of nationally coordinated criminal history check information from ACIC in respect of an Applicant as part of our fit2work services, you do so in accordance with the ACIC's National Police Checking Service Customer Terms of Use set out in schedule 2 to this SOW which governs those services. You warrant to us that you will comply with those terms, and that your privacy and data storage policies are consistent with those terms. Notwithstanding any other provision of this SOW, if we are not satisfied as to an Applicant's claimed identity or the legitimacy of the identity documents supplied for purposes of a search application to ACIC, and you cannot otherwise satisfy us as to such matters, we may refuse to lodge that application but still render a fee for the service.

4.5 Where you are placing an order for a fit2work service on behalf of an Authorised Client, you are permitted to use those services and any information provided to you as a part of those services for the sole purpose of providing your recruitment or other employment-related services to your Authorised Client, provided that you do not also use those services for your own benefit, and clause 4.2 of the Terms of Supply and clause 3.1 of this SOW are modified accordingly.

4.6 Where you are placing an order for a fit2work service on behalf of an Authorised Client, you:
(a) warrant that you have authority to act as the agent of the Authorised Client;
(b) will ensure that the Authorised Client complies with this agreement (including clauses 3.1 and 3.2 of this SOW) as if it were a party hereto;
(c) will be responsible for the acts and omissions of your Authorised Client in your own right and as if they were your acts or omissions;
(d) indemnify us in accordance with clause 10.7 of the Terms of Supply in respect of any loss or liability we incur through any acts or omissions of your Authorised Client.

4.7 You undertake that:
(a) you or your Authorised Client (as relevant) will provide the Applicant with a reasonable opportunity to respond to or validate the information contained in any report provided by either the ACIC or the AFP before making any decisions that may adversely affect that Applicant; and
(b) if an Applicant wishes to formally dispute the accuracy of any report provided by either the ACIC or the AFP, you will refer that Applicant to us to enable use of an appropriate 'Disputed Record' form and consideration by that authority, prior to you relying on any of the information contained in that report.

4.8 Where you place an order for the provision of KYC / AML checks, you acknowledge that we are not a reporting entity, nor providing a designated service, as contemplated by an AML/CTF Act, and our services do not relieve you of your obligations under that legislation.

4.9 Where you access our fit2work services through or at the direction of a reseller or other third party, we may pay that third party a commission or provide benefits to it for enabling that use of our information services.

5. Information we collect from and provide to you

5.1 We will comply with all applicable Privacy Laws;
(a) only collect, use and disclose personal information required to provide the fit2work services in accordance with the Collection Statement accessible electronically at *www.equifax.com.au/hrsolutions/pdf/fit2work-collection-statement.pdf*, as made available to any Applicant;
(b) be responsible for ensuring that any sub-contractors engaged by us in providing the fit2work services are also compliant with this our obligations under this SOW;
(c) hold data provided by you or an Applicant securely and take all appropriate steps to prevent:
(i) misuse, interference and loss; or
(ii) unauthorised access, modification or disclosure, of that data,
and will advise you:
(iii) if we receive a complaint about the handling of that data;
(iv) the steps taken to resolve any such complaint;
(v) if there is a data breach or incident involving that data; and
(vi) the steps being taken by us to remedy any such breach or incident and to prevent it from re- occurring; and
(d) if you request, permit you undertake annual privacy and security reviews to monitor compliance with this clause 5.1 of the SOW in respect of your data.

5.2 We are not in any way providing advice to you in respect of your obligations under, or your compliance (or otherwise) with, any Law, and we disclaim all responsibility for any use you may choose to make of the fit2work services in assisting you to comply with any Law. For example, if you seek a National Police Check from the AFP, you must be satisfied as to any relevant Commonwealth legislation or other basis supporting that check.

5.3 Without limiting clause 5.1 of this SOW, other than as may be required by Law or for a secondary purpose disclosed to the Applicant (and, if that use involves direct marketing, that Applicant has not 'opted-out'), we hold personal information submitted by an Applicant for a minimum of 3 months but no longer than 15 months after a check is completed. We hold any report generated by us for you for at least 2 years after its provision to you.

5.4 We seek to collect and supply the personal information of an Applicant through upload to our website. Where you or the Applicant choose to provide or receive personal information by e-mail, both you and the Applicant acknowledge that e-mail is not a secure form for transmitting information and that any communications transmitted over it may be intercepted or accessed by unauthorised or unintended parties, may not arrive at the intended destination or may not arrive in the form transmitted. In such circumstances, we take no responsibility for communications transmitted over the internet and give no assurance that such communications will remain confidential or intact. Any such communications shall be at the sole risk of you and the Applicant. Where our information services are accessed or viewed by means or in formats other than as originally intended or provided by us, both you and the Applicant remain responsible for reviewing all pertinent portions of those services, including any relevant disclosures and disclaimers.

5.5 Without limiting clause 3.7 of this SOW or clause 5.2 of the Terms of Supply, you acknowledge that:
(a) the results of a check may be constrained by data fields that are collected by a data provider (such as bankruptcy checks under an Insolvency Register) and an exact match to an Applicant may not be possible, in which case we will report a 'possible match';
(b) if an Applicant refuses permission to contact a specific prior employer or contractor, we may rely on secondary evidence (such as a payslip provided by the Applicant) to complete a check; and
(c) we can provide no assurance as to the legitimacy of any prior employer, educational institution, professional membership body or like entity as identified by an Applicant,
and we do not provide any guarantee or warranty as to the accuracy or completeness of any data returned to you or to third parties.

5.6 Upon request, we will promptly provide you with information held by us under a fit2work service agreement in relation to the COVID-19 vaccination status of a relevant Applicant.

6. Fees

6.1 Unless otherwise covered by a Fee Schedule, you must pay us the fees for our fit2work services as displayed and accessible electronically at **https://www.equifax.com.au/fit2work/** when you access the relevant service.

6.2 In addition to the fees identified by clause 6.1 of this SOW (and unless otherwise provided by a Fee Schedule), we will:
(a) charge additional fees for searches we conduct outside of Australia and New Zealand: those additional fees will be based on the country and type of verification requested and we will notify you of any such additional fees and seek your consent before proceeding with the relevant search; and
(b) pass through any disbursements levied by third party information providers such as academic institutions, agencies, professional bodies and like entities, but capped at $250 per Applicant search.

6.3 The Fee Schedule may specify a 'Term' as the duration for our information services. Where that period expires, and no further duration is identified, the information services can continue or repeat indefinitely.

6.4 We may charge you a fee when you order one or more fit2work checks on an applicant (excluding medical checks) and the check(s) are cancelled before completed, or if an incomplete ordered check remains open for more than ninety (90) days from the date of order. The fee is reflected in the Fee Schedule or in our communications with you. This fee is not intended to exclude, limit or modify a Consumer's rights described in clauses 2.1 and 2.2 above.

7. Privacy

7.1 Notwithstanding that, in providing our information services to you:
(a) we act as your agent under a limited agency in accordance with the Terms of Supply; and

(b) you may have notified us of a privacy policy or any other privacy statement that you operate under, the fit2work services are supplied in accordance with our Privacy Statement, accessible electronically at www.equifax.com.au/hrsolutions/pdf/privacy.pdf, and this SOW. You warrant that our delivery of the fit2work services is compatible with the privacy policy or any other privacy statement or requirement that you operate under.

8. Onboarding Form

8.1 Where you are a new customer, you establish and accept your contractual arrangements with us by completing an Onboarding Form and submitting that to us. Upon approval of that request we will create an account in your name. You represent and warrant that all information provided to us in that Onboarding Form, including the information identifying and relating to any Authorised Officer you specify from time to time, is true, correct, accurate and not misleading and sufficient to allow us to properly assess both your business eligibility and the appropriateness of that Authorised Officer.

8.2 Notwithstanding clause 8.1 and any absence of a completed Onboarding Form, by ordering and accepting our fit2work services (and in the absence of any other specific contractual arrangements between us) you agree those are delivered on the terms in this SOW and the Terms of Supply.

8.3 You acknowledge that ACIC, other governmental departments or supplier entities may require us to satisfy ourselves:

(a) as to the identity of an Authorised Officer; and

(b) that any Authorised Officer is a 'fit and proper' person, or otherwise appropriate, for purposes of that role, and agree that we may obtain a nationally coordinated criminal history check information from ACIC in respect of an Authorised Officer (together with any other check or checks we may determine as appropriate, acting reasonably) as part of our fit2work services for you, at such times and from time to time as we may determine prudent to satisfy our obligations to that data supplier.

8.4 Without limiting clause 9 of the Terms of Supply, where your Authorised Officer acts in that capacity for purposes of any nationally coordinated criminal history check sourced through ACIC, you will ensure that they deal with such information only as permitted by the terms of schedule 2 (NPCS Services) to this SOW (including clause 10 of that schedule). You acknowledge that the obligations under this clause 8.4 survive the expiry or termination of our agreement and exist in perpetuity, unless otherwise notified by us or ACIC.

8.5 Further guidance on the obligations of an Authorised Officer in connection with any nationally coordinated criminal history check sourced through ACIC is accessible electronically (after logging in) in our toolbox at fit2work.com.au. To the extent that there may be any inconsistency between that guidance and schedule 2 (NPCS Services) to this SOW, the latter prevails.

9. Document verification – Gateway Service User

9.1 Where you wish to access a Gateway Service enabling you to direct information match requests to and from a document issuer or Official Record Holder, we may facilitate provision of those services through a related body corporate.

9.2 Where a Gateway Service is provided to you, you acknowledge and agree:

(a) to comply with the DVS Terms and Conditions of Use set out in Schedule 3;

(b) to comply with any reasonable instructions regarding the use of the Gateway Service;

(c) that we have no responsibility for your use of that Gateway Service;

(d) that you access the Gateway Service under a separate contract with our related body corporate, including through complying with any further terms and conditions of use as may be imposed by the Gateway Service hub; and

(e) you will create or modify your business processes and ICT security in a manner reasonably acceptable to that company to establish and maintain functional connection to the hub.

10. Medical checks

10.1 Our medical check information service fees are based on use of Jobfit, our primary medical service provider, in accordance with clause 10.2 of this SOW. Those fees may change in accordance with clause 7.5 of our Terms of Supply. If we determine to use, or you request that we use, another medical check service provider, additional or different fees may apply. For example, we may determine to use another provider if Jobfit does not have capacity, where the Applicant is in a remote regional location or to meet a specific timeframe. We will notify you through our platform when making a booking with another provider and, where practicable, will advise you of any additional or different fees that may apply.

10.2 You will request any medical assessment for an Applicant as a fit2work service through our platform. When using Jobfit, this will permit the flow of relevant information to populate the Jobfit MediManager system and Jobfit will contact the Applicant to co-ordinate any appointment for the medical assessment. Status updates will be available to you through our fit2work platform.

10.3 Irrespective of the service provider, certain circumstances may require an additional medical assessment appointment to be made or additional costs to be incurred in respect of an Applicant. These circumstances include:

(a) multiple health practitioners are required to complete all requested check assessments;

(b) an Applicant is not able to attend the initial appointment and so needs rebooking;

(c) an Applicant cancels their appointment with less than **one clear working days' notice** through the Jobfit MediManager system (or otherwise to us), fails to attend their appointment at the

scheduled time, or requires extra services to be performed to achieve the assessment sought;

(d) certain aspects of the medical assessment not being able to be conducted at the initial appointment or needing to be undertaken at a different clinic; for example, if an instant drug screen result is non-negative, an additional GCMS test may be required to confirm the result – in which case an additional fee will apply, dependant on the pathology clinic used.

10.4 Where clause 10.3 of this SOW applies, further fees apply for the additional administrative work undertaken, as well as any additional clinic or similar fees incurred. If an Applicant cancels their appointment with less than one clear working days' notice, a cancellation fee equaling 100% of the fee for that medical assessment will apply. Any such additional fees may be rendered by a second invoice, credit or adjustment note from us. We will provide an appropriate explanation of those costs at the time of rendering for such additional fees and costs.

10.5 If a practitioner requires further information (whether from an Applicant's GP or otherwise) to perform the required medical assessment on an Applicant, the Applicant must provide that directly to the doctor. In such circumstances:

(a) we will not receive that further information and, if it is misdirected to us, we will treat it as unsolicited personal information and destroy it as soon as practicable; and

(b) any associated costs in obtaining that information are to be paid by the Applicant – it is then at your discretion as to whether to reimburse the Applicant for those costs.

Where an Applicant does not provide information requested by a practitioner within 2 weeks of the initial appointment, the Applicant's check will be closed as "incomplete" and our fees will apply.

10.6 In relation to the provision of COVID-19 vaccination status evidence and any other corresponding information relevant to COVID-19 vaccination provided by you or an Applicant to us, you warrant that you have conducted your own assessment and satisfied yourself as to whether you can legally request the evidence or corresponding information from the Applicant and authorise us as your agent to collect such information on your behalf.

11. Bankruptcy checks

11.1 You acknowledge and agree that prior to requesting for a bankruptcy check, you agree to provide any notification to individuals or obtain any consents that are required under the Privacy Law to request for the bankruptcy check.

11.2 The bankruptcy check will be conducted on the information, being the full primary name and date of birth, that is declared in the fit2work platform provided by the Applicant. Accordingly, you acknowledge and agree that by not providing the Applicant's full primary name (including middle name where applicable) or providing false or incorrect information, may result in a bankruptcy check that is incomplete or incorrect.

11.3 Further to clause 11.2, the Applicant will ultimately be responsible for providing the information that will be used to conduct the bankruptcy check. In any event:

(a) we do not independently verify the information that has been declared in the fit2work platform by the Applicant or you;

(b) we take no liability for any incorrect or incomplete bankruptcy check caused by you or the Applicant providing incomplete or incorrect information; and

(c) we do not provide any guarantee or warranty as to the accuracy or completeness of any information provided to you or the Applicant.

12. Confidential Information

Where you are aware of any suspected or actual breach of clause 9 of the Terms of Supply, you must notify us immediately and take all reasonable steps to prevent or stop the suspected or actual breach.

13. Intellectual Property

12.1 In order for us to provide you with the fit2work services under this SOW, we may incorporate data obtained from third-party sources including (but not limited to) AHPRA Data into the fit2work services.

12.2 In addition to clause 8 of the Terms of Supply, you acknowledge and agree that the Intellectual Property Rights in the data outlined in clause 12.1 of this SOW will remain the sole property of the party that provided the data.

12.3 Nothing in this SOW assigns, grants or transfers any right, title or interest in the data outlined in clause 12.1 of this SOW, to you.

Schedule 1 – Dictionary

In this fit2work SOW:

(a) "ACC Act" means the *Australian Crime Commission Act 2002* (Cth);

(b) "Account Representative" means an officer appointed by us and notified to you as our primary point of contact for your dealings with us;

(c) "ACIC" means the Australian Criminal Intelligence Commission;

(d) "Accredited Body" means an accredited body under section 46A(5) of the ACC Act having an agreement with ACIC permitting it to access the National Police Checking Service;

(e) "AFP" means the Australian Federal Police;

(f) **AHPRA Data** means health practitioner registration data obtained from the Australian Health Practitioner Regulation Agency and incorporated or uploaded into the eCredential platform and provided as part of the eCredential Services.

(g) "AML/CTF Act" means, as relevant, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) or *Anti- Money Laundering and Countering Financing of Terrorism Act 2009 (*NZ);

(h) "Approved Purpose" means:

(i) the use of our fit2work information services for pre-employment and employment screening in accordance with the consent given to you by the relevant Applicant; or

(ii) such other purpose as we may expressly agree with you in writing;

(i) "Authorised Client" means, where you act as an agent or service provider to provide recruitment or other employment- related services or real estate services to a third party who is your customer or to whom you otherwise provide a service, that person;

(j) "Authorised Officer" means the officer appointed, or deemed to be appointed, by you under clause 3.1 of this SOW and as specified in an Onboarding Form or any updated advice to us;

(k) "Commencement Date" means the date you establish account arrangements with us to use our fit2work services;

(l) "Consumer" has the same meaning as given by the Consumer Law;

(m) "deal" includes collecting, recording, holding, organising, storing, adapting, altering, retrieving, consulting, using, disclosing, transferring, providing access, combining, blocking, erasing or destroying and "dealing" has a corresponding meaning;

(n) "employer" means the entity that employs or otherwise retains you, or may employ or otherwise retain you, where that entity has obtained your consent to the collection of your personal information for purposes of a relevant information service, and includes:
(i) any entity retaining or seeking to retain your services under contract or other similar service arrangement;
(ii) an entity in which you are, or are seeking to become, enrolled or a member (including any educational, social or charitable institution): and
(iii) where relevant, an Authorised Client;

(o) "EU" means that organisation of European countries known as the 'European Union' having joint policies on matters such as trade, agriculture and finance;

(p) "fit2work Badge" means that fit2work service providing a profile badging system to a Consumer Applicant, allowing them to share their verified credentials with employers through allocation of a unique ID number that can be verified independently via the fit2work website;

(q) "fit2work services" means our supply of any of the information services described in clause 1.5 of this SOW;

(r) "Gateway Service" means a service that enables authorised users to connect to and interact with document issuers or Official Record Holders through an intermediary hub;

(s) "GDPR" means the General Data Protection Regulation as created by the European Commission;

(t) "Home Affairs" means the Commonwealth of Australia represented by the Department of Home Affairs ABN 33 380 054 835;

(u) "Insolvency Register" means, as relevant, the *National Personal Insolvency Index* maintained by the Australian Financial Service Authority or the *Insolvency Register* maintained by Records NZ;

(v) "Jobfit" means Jobfit Health Group Pty Ltd ABN 40 083 014 340 and includes any Affiliates or contractors working on its behalf;

(w) "MoJ" means the Ministry of Justice (Tāhū o te Ture) in New Zealand;

(x) "Official Record Holder" means, in respect of a supported document, the entity against whose official record data the information submitted is requested to be matched (or attempted to be matched);

(y) "Onboarding Form" means an application to us, completed by you in the form we provide to you; and

(z) "Privacy Legislation" means the Privacy Act, any regulations, directives or other subordinate legislation made under a Privacy Act, and any other legislation applying in Australia (including of the Commonwealth of Australia or any State or Territory of Australia) or in New Zealand from time to time affecting privacy, personal information or the collection, handling, storage, processing, use or disclosure of personal information (including health information), data and other types of information and includes the *Spam Act 2006* (Cth), *Do Not Call Register Act 2006* (Cth), *Commonwealth Electoral Act 1918* (Cth), the *Telecommunications Act 1997* (Cth) and the *Unsolicited Electronic Messages Act 2007* (NZ), regardless of whether those Laws would apply to you but for this agreement.

Schedule 2 — National Police Checking Service Customer Terms of Use

1. **The Service**
    a. The Australian Criminal Intelligence Commission (ACIC) administers access to nationally coordinated criminal history checks under the *Australian Crime Commission Act 2002* (Cth) (**ACC Act**).
    b. Entities requesting a nationally coordinated criminal history check can only do so through a body that has been accredited by the ACIC CEO for the purposes of receiving nationally coordinated criminal history checks under s. 46A(5) of the ACC Act (the **Accredited Body**).

2. **Acceptance of the Terms of Use**
    a. To use the Service, you confirm your acceptance and commitment to complying with the terms and conditions set out in these Terms of Use for Controlled Access to Nationally Coordinated Criminal History Checks (**Terms of Use**).
    b. These Terms of Use are entered into by you in favour of the Accredited Body (Fit2Work) and the ACIC.

3. **Your obligations as customer**
    a. You acknowledge that you may submit requests for nationally coordinated criminal history checks for your current and prospective Personnel and that you will only be entitled to receive the check results report for applications submitted for these Personnel.
    b. You understand and acknowledge that you will not be operating in a commercial capacity in relation to nationally coordinated criminal history checks nor will you provide nationally coordinated criminal history checks to third parties, whether in exchange for a fee or for any other purpose, unless authorised or required by law.
    c. You agree to treat any information provided to you by the Accredited Body confidentially and comply with the provisions of the Privacy Act 1988 (Cth) when dealing with any Personal Information or Police Information provided to you as part of the Service and undertake to secure all such information against loss and unauthorised access, use, modification or disclosure.
    d. You can only use Personal Information and Police Information for the purpose as consented to on the application form.
    e. You must not transfer, access or store any of the Personal Information or Police Information outside Australia, without first consulting with the ACIC.
    f. ACIC reserves its right to refuse any request to transfer, access or store Personal Information or Police Information offshore if any such transfer, access or storage is in contravention to the terms of the agreement for controlled access to nationally coordinated criminal history checks between the ACIC and the Accredited Body.

4. **Limitations of the Service**

    A nationally coordinated criminal history check is a point in time record. If you need to request a nationally coordinated criminal history check for an Applicant after 3 months have passed since a prior nationally coordinated criminal history check was issued for that Applicant, you will need to submit a new nationally coordinated criminal history check application.

5. **No representation or guarantee**
    a. You acknowledge and agree that the ACIC makes the information contained in a nationally coordinated criminal history check, including a check results report, available for use on the following conditions:
        i. the ACIC makes no representation or warranty of any kind in respect to its accuracy; and
        ii. the ACIC does not accept responsibility or liability for any omission or error in the information.
    b. You further acknowledge that the ACIC is not responsible for, and is not liable for any loss, liability or expense arising from:
        i. the checking or vetting of convictions which may be spent prior to their disclosure to you via the Service; or
        ii. any information that is released to you contained within a check results report.

6. **Defined terms**

    In these Terms of Use, the following definitions are used:
    a. **Applicant** means a natural person in relation to whom a nationally coordinated criminal history check is sought;
    b. **Application** means a form (in physical or electronic format) completed by the Applicant, or on behalf of the Applicant, submitted to the Accredited Body and provided to the ACIC, requesting the ACIC to conduct a nationally coordinated criminal history check in relation to the Applicant;
    c. **Check Results Report** means a report in a physical or electronic format outlining the results of a nationally coordinated criminal history check provided by the ACIC to the Accredited Body as a result of the Accredited Body accessing and using the Service;
    d. **Law** means any applicable statute, regulation, by-law, ordinance or subordinate legislation in force from time to time in Australia, whether made by the Commonwealth, a State, Territory or a local government, and includes the common law and rules of equity as applicable from time to time;
    e. **Personnel** means all existing and prospective individuals employed or engaged by you, including in a volunteer capacity;
    f. **Personal Information** has the meaning given in the *Privacy Act 1988* (Cth);
    g. **Police Information** means any of the following information:
        i. information collected for the purposes of providing the Service;
        ii. information collected for the purposes of a nationally coordinated criminal history check; and
        iii. information released as part of a nationally coordinated criminal history check including any information accessible for the purposes of the Service, including in a Check Results Report;
    h. **Service** means the National Police Checking Service.

Schedule 3 – DVS Services

Document Verification Service Business User
TERMS AND CONDITIONS OF USE

Introduction

1. Your access to and use of the DVS is subject to these Document Verification Service Business User Terms and Conditions of Use (these Conditions).

Use or disclosure of Any Australian Government Related identifier

2. You must not use or disclose an Australian Government Related Identifier of an individual unless:
   2.1. the use or disclosure of the identifier is reasonably necessary for you to verify the identity of the individual for the purposes of your activities or functions; or
   2.2. the use or disclosure of the identifier is reasonably necessary for you to fulfil your obligations to an Agency or an Australian State or Territory Authority; or
   2.3. the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order.
3. You acknowledge that, where you are subject to the Australian Privacy Act, a breach of clause 2 would also involve a breach of Australian Privacy Principle 9.2.

Pre-conditions to DVS use

4. To be able to connect to the DVS you must:
   4.1. be carrying on a business in Australia and/or New Zealand;
   4.2. have an operational DVS Business User ID;
   4.3. either yourself be a current Approved Gateway Service Provider or have in place an arrangement with a third party current Approved Gateway Service Provider;
   4.4. ensure any DVS Information Match Results you receive are recorded so as to allow the DVS Manager to efficiently and effectively audit your compliance with these Conditions; and
   4.5. meet all other requirements the DVS Manager may advise you of relating to your access and use of the DVS.
5. You represent and warrant all information provided to the DVS Manager and to your Approved Gateway Service Provider by any means and at any time, including in, or in relation to, any application in relation to your access to or use of the DVS to use the DVS, is true, correct, accurate and not misleading.
6. You acknowledge and agree that you will be legally bound by and must observe the Document Verification Service Business User Terms and Conditions of Use (which you have acknowledged that you have received, read and understood prior to contracting with your Approved Gateway Service Provider) as and from the date the DVS Manager advises you in writing that you have been registered as an 'Approved Business User'.
7. You further acknowledge and agree that in consideration of Austroads and Registries of Births, Deaths and Marriages (BDMs) agreeing with Home Affairs to provide Information Match Results in relation to State and Territory document information in connection with the Document Verification Service and to perform other obligations to the DVS Manager, as and from the time you first issue an Information Match Request in respect of a State or Territory Supported Document you will be legally bound by and must observe the Document Verification Service Business User Terms and Conditions of Use under an additional and separate contract with Austroads and BDMs.
8. You acknowledge and agree that you will only seek access to, and you undertake only to use, address details from the Australian Electoral Commission, or any associated Information Match Results, for the purposes of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth) or the *Financial Transactions Reports Act 1988* (Cth).

Use

9. You must ensure that all your Personnel are aware of and comply with all provisions of these Conditions that are relevant to their role, function and duties.
10. You must ensure that your use of the DVS does not (and does not attempt to) modify, interfere with, disrupt, adversely affect or misuse the DVS or DVS functionality in any way, or interfere with or disrupt use of the DVS by any other person.
11. You must ensure that, your access to and use of the DVS (which includes submission of Information Match Requests) and your access to and use of Information Match Data complies with all laws, regulatory requirements, and complies with all codes of conduct to which you ascribe.
12. You must promptly provide the DVS Manager with any information the DVS Manager requests in respect to your access to or use of the DVS, including any routine reports and certifications.
13. You must strictly comply with all requirements, instructions and guidance the DVS Manager advises you in respect to your access to and use of the DVS and Information Match Data and any other related matter.
14. Your use of the DVS must at all times comply with all applicable laws, without limitation including all relevant Privacy Laws. Unless authorised in writing by the DVS Manager, you must not use or disclose any personal information obtained through your use of the DVS for any purpose other than your access and use of the DVS.
15. Except as may be specifically authorised by the DVS Manager in writing, you must:
   15.1. only access and use the DVS and DVS Data in Australia and / or New Zealand;
   15.2. not allow any person other than your authorised Personnel to access or use Information Match Data or your DVS Business User ID;
   15.3. only access and use the DVS and Information Match Data exclusively for your own internal purposes;
   15.4. not use the DVS or collect, store or use Information Match Data for any purpose associated with the provision, or potential provision of, an information service to any person;
   15.5. not use or disclose any personal information (as defined in relevant Privacy Laws), if any, contained in any Information Match Result or otherwise provided by the DVS Manager for any purpose other than your access and use of the DVS; and
   15.6. not make any public statement concerning the DVS or your access to or use of it.

   For any organisation outside Australia or New Zealand seeking to connect to the DVS, permission for access and use of the DVS must be sought in writing from the DVS Manager, as per clause 15. When seeking this permission, such organisations must specify the processes and procedures that they have in place to mitigate any risks, in terms of the handing of any personal information accessed on the DVS.
16. You must not, by act or omission, directly or indirectly, mislead any person in relation to the DVS, your access to or use of the DVS or any related matter.
17. You and your Approved Gateway Service Provider must fully cooperate with and support any audit or verification process the DVS Manager (or our agents) wishes to conduct to verify your compliance with these Conditions, without limitation including providing the DVS Manager with prompt access to relevant records, systems, premises and facilities. You authorise the DVS Manager access to any records or information held by any Approved Gateway Service Provider relevant to your access to or use of the DVS.

Privacy, consent and information use

18. You must ensure that your use of the DVS and Information Match Data complies with all relevant Privacy Laws.
19. You must ensure that each individual providing details in a Supported Document to you:

19.1. confirms they are authorised to provide those details to you;

19.2. is informed of the purpose for which that information is sought and will be used by you including that:

a. the information will be subject to an Information Match Request in relation to relevant Official Record Holder information;

b. that the Information Match Request, the Information Match Result and other Information Match Data and your access to and use of the DVS, may involve use of third party systems and services; and

c. as relevant, that information provided to or by you in or from Australia will be transmitted to New Zealand or vice versa,

and provides you with their express consent for such use and accessing such information, and as relevant, such transmission, prior to any such use or access or transmission being initiated or made by you and that you keep full and proper records of all such disclosures, confirmations and consents.

Your facilities

20. You must provide everything that you need to access and use the DVS and ensure that your equipment and facilities are properly configured and otherwise meets all relevant requirements advised by the DVS Manager.

Fees and charges

21. You must pay all fees and charges advised to you in respect to you being a DVS Business User. Unless specifically stated to the contrary, all fees, once incurred are payable and once paid are non-refundable, including where your access to or use of the DVS is cancelled, suspended or terminated for any reason.

Security

22. You must comply with all security procedures advised to you in relation to the DVS and take all reasonable action to protect and maintain the security of the DVS and your access to and use of it, including, without limitation, maintaining the security of all tokens, access codes, encryption keys and other information relating to access, authentication or security relating to the DVS.

23. You must take all reasonable action to prevent and detect unauthorised use of the DVS and your Business Access System.

24. You must immediately notify the DVS Manager if you know or suspect that access or authentication security information has been compromised or any other kind of unauthorised use or security breach has occurred, or if you know or suspect that there is a security vulnerability, fault, error or problem in the DVS or any Information Match Result.

Updates and changes to the DVS

25. The DVS may be upgraded and its features, functionality and other characteristics may change from time to time. The DVS Manager will endeavour to provide reasonable notice of any changes that the DVS Manager considers is not routine and should be advised to DVS Business Users. You acknowledge that it may not be reasonably possible to provide notice in all circumstances and that in no event will the DVS Manager be obliged to provide notice exceeding 14 days.

The DVS is provided 'as is' and 'as available'

26. The DVS has been implemented in a technical environment that is designed to provide high availability and be fault tolerant. However, as with any technology based facility, the speed and characteristics of the DVS will vary at different times and under different circumstances and the DVS may not always work as described, and the DVS and Information Match Results may be subject to faults, errors, interruption or breakdown or be fully or partially unavailable. You acknowledge and agree that, subject to clause 34, your access to and use of the DVS is on an 'as is, as available' basis only, and without limiting the foregoing:

26.1. you must ensure your business processes and operations can be satisfactorily conducted despite the DVS or Information Match Data being subject to faults, errors, interruption or breakdown or be fully or partially unavailable for any reason; and

26.2. any information the DVS Manager provides regarding availability, performance or other service levels or characteristics relating to the DVS, no matter how expressed, are non-contractual statements of intent only and do not constitute a representation or warranty of any kind.

27. You acknowledge and agree that you:

27.1. are solely responsible for your business processes and decisions;

27.2. must, where any issues arise with your customers or other stakeholders that in any way relate to your access to or use of the DVS or Information Match Data, ensure that the relevant customers and stakeholders understand that you are the sole point of contact in relation to those issues; and

27.3. must manage and resolve all such issues yourself as expeditiously as possible and without seeking to involve the DVS Manager in any way.

Changes to these conditions

28. The DVS Manager can update or otherwise vary these Conditions by not less than 45 days prior written notice to you.

Cancellation

29. The DVS Manager will promptly cancel your DVS Business User ID if you notify the DVS Manager to do so. The DVS Manager will advise you once cancellation has been effected.

Suspension and Termination

30. The DVS Manager may refuse access to the DVS, or suspend its operation in whole or in part either for you as a specific DVS Business User, for any Approved Gateway Service Provider or generally, at any time for any reason the DVS Manager thinks fit.

31. The DVS Manager may terminate your DVS Business User ID:

31.1. with or without cause at any time by not less than 45 days prior written notice to you; and

31.2. where you have breached these Conditions, immediately by written notice to you.

Indemnity

32. Subject to clause 35, you indemnify the DVS Manager against any loss, damage, cost, expense (including legal expenses on a solicitor and own client basis), claim, proceeding or liability of any kind that the DVS Manager (or our Personnel) may incur, that arises (no matter how arising including from negligence by the DVS Manager) out of or in connection with, your use (including unauthorised use) of your DVS Business User ID, your access to or use of the DVS and Information Match Data, the correctness or otherwise of Information Match Data, your Gateway Service or the lawful exercise of our rights pursuant to these Conditions.

Priority

33. To the extent of any inconsistency between a provision in this document and any other provision forming part of these Conditions, the provision in this document will prevail.

Disclaimer and liability

34. You acknowledge that we provide Information Match Results based on information provided to us by Official Record Holders and third parties and that we have not independently verified the accuracy or completeness of the information provided. Subject to clause 35, the DVS and Information Match Results are made available without any representation or warranty of any kind (without limitation in respect to the accuracy of Information Match Results) and the DVS Manager has no liability to you in respect of any loss or damage that you might suffer no matter how arising (including from negligence by the DVS Manager) that is directly or indirectly related to the DVS, or Information Match Data or any other relevant matter, without limitation including any Gateway Service and, any Approved Gateway Service Provider.

35. Except as set out in this clause 35, nothing in these Conditions excludes, restricts or modifies the application of, or liability in respect of, any consumer guarantee that applies to these Conditions under the Australian Consumer Law (Consumer Guarantee). Our liability for any failure by the DVS Manager to comply with a Consumer Guarantee that applies to these Conditions is limited to the DVS Manager (at our election):

35.1. supplying the services again; or
35.2. paying the cost of having the services supplied again,
except where it is not 'fair or reasonable' (as contemplated under section 64A of the Australian Consumer Law) for the DVS Manager to do so.

Notice

36. The DVS Manager may advise or notify you of any matter in relation to the DVS and these Conditions by email, mail, facsimile or telephone to any relevant address or number that you have provided to the DVS Manager.

Applicable law and jurisdiction

37. These Conditions are governed by, and are to be construed in accordance with, the laws of the Australian Capital Territory.
38. The DVS Manager and you irrevocably and unconditionally submit to the non-exclusive jurisdiction of the courts of the Australian Capital Territory and any courts that have jurisdiction to hear appeals from any of those courts and waives any right to object to any proceedings being brought in those courts.

Definitions

39. In these Conditions, unless the context implies a contrary intention, the following terms have the meaning set out below:

Agency means an *agency* as defined in the Australian Privacy Act.

Approved Gateway Service Provider means a provider of a Gateway Service that is at all relevant times approved by the DVS Manager.

Australian Consumer Law means Schedule 2 to the *Competition and Consumer Act* 2010 (Cth) and the corresponding provisions of the Australian Consumer Law (ACT) or any other state or territory as applicable.

Australian Privacy Act means the *Privacy Act 1988* (Cth)

Australian Government Related Identifier means a *government related identifier* as defined in the Australian Privacy Act (as at the date of publication of these Conditions being *an identifier of an individual that has been assigned by:*

a. a Commonwealth government agency
b. an Australian state or territory
c. an agent of a Commonwealth government agency, or an Australian state or territory authority, acting in its capacity as an agent, or
d. a contracted service provider for an Australian Commonwealth or state or territory contract, acting in its capacity as a contracted service provider for that contract).

Australian State or Territory Authority means a *State or Territory authority* as defined in the Australian Privacy Act.

Austroads means Austroads Ltd ACN 136 812 390.

BDMs means Registries of Births, Deaths and Marriages in Australian States and Territories.

Business Access System means systems and facilities that you use to connect to and interact with the DVS.

DVS means the system (including all associated services, infrastructure, applications, facilities, functionality, data, information and material, whether belonging to or operated by the DVS Manager or a third party) established by the DVS Manager to provide Information Match Results (but does not include any Gateway Service).

DVS Business User ID means a number or other mechanism (and associated access credentials) provided by the DVS Manager by which you are uniquely identified to the DVS Manager for purposes including accessing the DVS, transaction processing, and record keeping.

DVS Manager means Commonwealth of Australia acting and represented by the Department of Home Affairs and, in relation to clauses 25, 31, 33 and 34, also includes each Official Record Holder and (in the case of State and Territory information) Austroads and BDMs.

DVS Testing Environment means any system or facility the DVS Manager makes available to you for testing purposes.

Gateway Service means the services and facilities (forming part of your Business Access System) by which your internal systems connect to the DVS.

Home Affairs means the Department of Home Affairs acting for and representing the Commonwealth of Australia.

Information Match Data means data and information in or relating to Information Match Requests or Information Match Results.

Information Match Request means an electronic request to the DVS by a User (required to be submitted in a structured electronic format advised by the DVS Manager) to be provided with an Information Match Result in relation to the details of relevant information in a Supported Document.

Information Match Result means, in respect to an Information Match Request, an electronic response indicating that the information provided in the request either matches or does not match the relevant official record data, or that a system error has been encountered in trying to process that request.

New Zealand Privacy Act means the *Privacy Act 1993* (NZ).

Official Record Holder means, in respect of each Supported Document, the entity against whose official record data the information submitted in an Information Match Request is matched (or attempted to be matched) via the DVS.

Our means the DVS Manager.

Person includes a natural person, partnership, unincorporated or incorporated association, corporation or body politic.

personal information has the meaning defined in the relevant Privacy Law.

Personnel includes employees, officers, directors, contractors and agents.

Privacy Laws means the Australian Privacy Act; the New Zealand Privacy Act and any other law relating to privacy or personal information which you may be subject to.

Supported Document means a type of document (for example an Australian Passport or Australian Citizenship Certificate) that is supported by the Document Verification Service.

We and **Us** means Commonwealth of Australia acting represented by the Department of Home Affairs and, in relation to clauses 26, 32, 34 and 35 also includes each Official Record Holder and (in the case of driver's licence information) Austroads and BDMs.

User means each person (and, if relevant, each automated system) who can initiate an Information Match Request in relation to your DVS Business User ID.

You means the relevant DVS Business User, and, as the context admits, each relevant User.