DATA PRIVACY AND SECURITY ADDENDUM

This Addendum by and between Randstad Pty Limited ("Randstad") and ("the Service Provider"), amends the agreement between the parties (the "Agreement"), under which the Service Provider is providing Randstad and/or Randstad Stakeholders with certain services (the "Services").

The parties agree as follows:

1. Definitions

"end user" means the individuals authorised by Randstad to access and use the services provided by the Service Provider under the Agreement.

"Personal Data" means the data concerning an identified or identifiable natural person processed or to be processed by the Service Provider in the context of this Addendum/the Agreement

"securely destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) Or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of applicable Australian legislation and/or guidelines relevant to data categorised as Personal Data.

"security breach" means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store or dispose of data is breached, and in which Randstad Data is exposed to unauthorised disclosure, access, alteration, or use.

"services" means any goods or services acquired by Randstad from the Service Provider.

"Randstad Data" means data provided to the Service Provider by Randstad which includes all personally identifiable information of any Randstad Stakeholder and other information that is not intentionally made generally available by Randstad on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and Personal Data of any Randstad Stakeholder.

"Randstad Stakeholders" means the person or persons whose Personal Data will be processed in connection with the provision of the Services including but not limited to Randstad's candidates, employees, contractors and customers or prospective customers.

"Registered User" means an individual who creates a profile on and/or otherwise becomes a registered user of the Service Provider's platform, system or services.

"Territory" means Australia.

2. Rights and license in and to Randstad Data

2.1 The parties agree that as between them, all rights including all intellectual property rights in and to Randstad Data shall remain the exclusive property of Randstad, and the Service Provider has a limited, nonexclusive license to use these data as provided in the Agreement solely for the purpose of performing its obligations hereunder. This agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the agreement.

2.2 The parties acknowledge and agree that once a Randstad Stakeholder or any other individual becomes a Registered User:

a) the Registered User is subject to the Service Provider's standard user terms and conditions and privacy policy as applicable from time to time; and

b) the Service Provider will be responsible for that individual's Personal Data in accordance with its own terms and conditions and privacy policy.

3. Intellectual property disclosure/rights

3.1 Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by the Service Provider (or its subcontractors) exclusively for Randstad under the Agreement will not be disclosed to any other person or entity without the written permission of Randstad.

3.2 The Service Provider warrants to Randstad that Randstad will own all rights, title and interest in any

intellectual property created by Randstad in connection with the Randstad Data as part of the performance of the Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. The Service Provider agrees to assign and hereby assigns all rights, title, and interest in any and all intellectual property created by Randstad as part of the performance of the Agreement to Randstad, and will execute any future assignments or other documents needed for Randstad to document, register, or otherwise perfect such rights. Nothing in this section is, however, intended to or shall be construed to apply to existing intellectual property created or owned by the Service Provider that Randstad is licensing under the Agreement or that the Service Provider creates or develops independently of its obligations under the Agreement. For avoidance of doubt, Randstad asserts no intellectual property ownership under this clause to any pre-existing intellectual property of the Service Provider, and seeks ownership rights only to the extent the Service Provider is being engaged to develop certain intellectual property exclusively for Randstad as part of its services for Randstad.

4. Data privacy

4.1 The Service Provider will only use or process the Randstad Data for the purpose of fulfilling its duties under the Agreement and in accordance with the specific processing instructions contained in Annex 1 or as otherwise instructed by Randstad in writing and is not entitled to perform operations in relation to the Randstad Data for which no instruction has been given. The Service Provider will in no event process Randstad Data for any purpose other than that determined by Randstad.

4.2 The Service Provider will not share Randstad Data or disclose it to any third party without the prior written consent of Randstad, except as required by the Agreement or as otherwise required by law and in that event pursuant to Clause 9.1 below.

4.3 The Service Provider will provide access to Randstad Data only to its employees and subcontractors who need to access the data to fulfill the Service Provider's obligations under the Agreement. The Service Provider will ensure that employees who perform work under the Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Addendum.

4.4 Randstad Data will not be stored outside the Territory without prior written consent from Randstad. The Service Provider's processing of Personal Data will comply with the local laws and regulations applicable in the Territory. Where applicable local law provides for a lower level of protection of Personal Data than that described in this Addendum, the requirements of this Addendum shall apply. Randstad acknowledges that the Service Provider uses third party service providers and that for some (eg Email delivery) this may involve Randstad Data being transmitted through networks and servers located outside of the Territory.

5. Data security

5.1 The Service Provider will store and process Randstad Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorised access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Service Provider's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

5.2 Without limiting the foregoing, the Service Provider warrants that in respect of the delivery of the Services under the Agreement, it has implemented the following with respect to its software platform and will guarantee these during the term of the Addendum/Agreement:

a) an information security management system that uses external service providers who are certified compliant with ISO27001/2:2013; or

b) all the security measures contained in annex II.

6. Employee background checks and qualifications

6.1 The Service Provider shall ensure that its employees who will have potential access to Randstad Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of the Agreement.

7. Data authenticity and integrity

7.1 The Service Provider will take reasonable measures, including audit trails, to protect Randstad Data

stored with the Service Provider against deterioration or degradation of data quality and authenticity but will have no responsibility for any actions of any Randstad employee or end user or any firm as may be appointed by Randstad to migrate any Randstad Data which cause any such deterioration or degradation. Any such selected firm selected by Randstad must be notified to the Service Provider in writing and be acceptable to the Services Provider acting reasonably, and will be responsible during the term of the Agreement, unless otherwise specified elsewhere in this Addendum, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

8. **Security breach**

8.1 Upon becoming aware of a security breach with respect to the Service Provider's system or services which has or would be reasonably likely to have a material adverse effect on Randstad, or of circumstances that are reasonably understood to suggest such a security breach is likely, the Service Provider will timely notify Randstad consistent with applicable local law, fully investigate the incident, and cooperate fully with Randstad's reasonable investigation of and response to the incident. Except as otherwise required by law, the Service Provider will not provide notice of the incident directly to individuals whose personally identifiable information was involved, regulatory agencies, or other entities, without prior written permission from Randstad.

8.2 If the Service Provider must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Randstad Data known as Personal Data then in addition to any other remedies available to Randstad under law or equity the Service Provider will:

a) reimburse Randstad in full for all reasonable costs incurred by Randstad in investigation and remediation of any security breach caused by the Service Provider with respect to such Personal Data, including but not limited to providing notification to individuals whose Personal Data was compromised and to regulatory agencies or other entities as required by law or contract;

b) the payment of reasonable legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the security breach.

8.3 If the Service Provider will under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Randstad Data known as Personal Data, then in addition to any other remedies available to Randstad under law or equity, the Service Provider will reimburse Randstad in full for all costs reasonably incurred by Randstad in investigation and remediation of any security breach caused by the Service Provider.]

9. **Response to legal orders, demands or requests for data**

9.1 Except as otherwise expressly prohibited by law, the Service Provider will:

a) promptly notify Randstad of any subpoenas, warrants, or other legal orders, demands or requests received by the Service Provider seeking Randstad Data;

b) reasonably consult with Randstad regarding its response;

c) cooperate with Randstad's reasonable requests in connection with efforts by Randstad to intervene and quash or modify the legal order, demand or request; and

d) upon Randstad's request, provide Randstad with a copy of its response.

9.2 If Randstad receives a subpoena, warrant, or other legal order, demand (including request pursuant to applicable laws) or request seeking Randstad Data maintained by the Service Provider, Randstad will promptly provide a copy to the Service Provider. The Service Provider will promptly supply Randstad with copies of data required for Randstad to respond, and will cooperate with Randstad's reasonable requests in connection with its response.

10. **Data transfer upon termination or expiration**

10.1 Upon termination or expiration of the Agreement, the Service Provider will ensure that all Randstad Data is securely returned or destroyed as directed by Randstad in its sole discretion. Transfer to Randstad or a third party designated by Randstad shall occur within a reasonable period of time, and without significant interruption in service. the Service Provider shall use reasonable efforts to facilitate that such transfer/migration adopts a standard format that as is reasonably agreed between the parties and

compatible with the relevant systems of Randstad or its transferee, and to the extent technologically feasible, that Randstad will have reasonable access to Randstad Data during the transition. In the event that Randstad requests destruction of its data, the Service Provider agrees to securely destroy all data in its possession and in the possession of any subcontractors or agents to which the Service Provider might have transferred Randstad Data. The Service Provider agrees to provide reasonable documentation of data destruction to Randstad.

10.2 So far as is reasonably practicable, the Service Provider will notify Randstad of impending cessation of its business and any contingency plans, and will use all reasonable endeavours if necessary to provide Randstad with reasonable access to the Service Provider's system to remove and destroy exclusively Randstad-owned assets and data. Where applicable, the Service Provider shall use all reasonable endeavours to implement its exit plan and take all reasonable actions to ensure a smooth transition of service with minimal disruption to Randstad. Where applicable, the Service Provider will work closely with its successor to ensure a successful transition to the system (where reasonably practicable), with minimal downtime and effect on Randstad, and where reasonably practicable all such work to be coordinated and performed in advance of the formal, final transition date.

11. **Audits**

11.1 The Randstad reserves the right in its sole discretion to perform audits of the Service Provider at reasonable times and on providing reasonable prior notice at Randstad's expense to ensure compliance with the terms of the Agreement. The Service Provider shall reasonably cooperate in the performance of such audits, provided that no such audit will disrupt the business carried on by the Service Provider or any services provided by the Service Provider to any of its customers. This provision 11.1 applies to all agreements under which the Service Provider must create, obtain, transmit, use, maintain, process, or dispose of Randstad Data.

11.2 If the Service Provider must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of Randstad Data which contains Personal Data or financial or business data which has been identified to the Service Provider prior to the date of this Addendum as having the potential to affect the accuracy of Randstad's financial statements, the Service Provider will at its expense conduct or have conducted no more than once annually:

a) security audit with reasonable audit objectives deemed sufficient by Randstad, which attests the Service Provider's security policies, procedures and controls;

b) vulnerability scan of the Service Provider's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement; and

c) formal penetration test of the Service Provider's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement.

11.3 Additionally, the Service Provider will provide Randstad upon reasonable request the results of the above audits, scans and tests, and where a reasonable request is made by Randstad will modify its security measures as needed based on those results in order to meet its obligations under the Agreement. Randstad may require, at Randstad's expense, the Service Provider to perform additional reasonable audits and tests, the results of which will be provided promptly to Randstad following payment by Randstad to the Service Provider of the Service Provider's costs or expense in performing any such audit or test.

12. **No Surreptitious Code**

12.1 The Service Provider warrants that, to the best of its knowledge, the software platform licenced to Randstad by the Service Provider under the Agreement is free of and does not contain any code or mechanism that collects information or asserts control of any system operated or owned by Randstad without Randstad's consent, or which may restrict Randstad's access to or use of Randstad Data as held by Randstad independently outside of that software platform. The Service Provider further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorised access to Randstad Data, or which may restrict Randstad's access to or use of Randstad Data as held by Randstad outside of any software platform or system operated by the Service Provider.

13. **Compliance**

13.1 Each of the Service Provider and Randstad will comply with all applicable laws and industry standards in

performing their obligations under the Agreement. Any of the Service Provider's or Randstad's personnel visiting the other party's facilities will comply with all applicable policies regarding access to, use of, and conduct within such facilities. Each such party will provide copies of such policies to the other party upon request.

13.2 The Service Provider warrants that the Services are fully compliant with relevant laws, regulations, and guidance that may be applicable to the service in the Territory.

14. **Survival; Order of Precedence, Governing Law**

14.1 This Addendum shall survive the expiration or earlier termination of the Agreement. In the event the provisions of this Agreement conflict with any provision of the Agreement, or the Service Providers' warranties, support contract, or service level agreement, the provisions of this Addendum shall prevail to the extent of the conflict or inconsistency.

14.2 This Addendum is governed by the laws of the State of NSW. Disputes will be submitted to the competent court in in that place.

Signed for and on behalf of:	Signed for and on behalf of **Randstad Pty Limited**:
Authorised Signatory: Name: Title:	Authorised Signatory: Name: Title:

Annex 1: Specific Processing Instructions

(as stated in each purchase order or similar)

Annex 2: Security measures

The parties acknowledge and agree that for the purpose of this Annex 2, 'Personal Data' refers to Personal Data of any Randstad Stakeholder provided to the Service Provider by Randstad which Randstad Stakeholder has not yet become a Registered User.

1. Access control to data center premises and facilities (physical)

1.1 Service Provider will maintain commercially reasonable physical security systems at all Service Provider sites which are used to Process Personal Data;
1.2 Physical access control will be implemented for all data centers. Unauthorized access is prohibited by onsite staff, biometric scanning or security camera monitoring at all times (24 hours per day, seven days per week);
1.3 Service Provider will maintain procedures for issuing identification markers or badges to authorized staff and controlling physical access to data centers under its control which process Personal Data;
1.4 Turnstiles will be integrated with access control readers to control physical access at all data center sites at all times by requiring staff to present a photo identity card prior to entering such an Service Provider site;
1.5 Visitors must be pre-approved before coming to such Service Provider sites which are used for to Process Personal Data and will be required to present identification, sign a visitor log, and be escorted at all times while on the sites.

2. Access control to systems (virtual)

2.1 Service Provider will establish and maintain all commercially reasonable safeguards against accidental or unauthorized access to, destruction of, loss of, or alteration of the Personal Data on its systems which are used to Process Personal Data:
2.1.1 access will be granted to personnel through documented access request procedures. The employees' managers or other responsible individuals must authorize or validate access before it is given;
2.1.2 access controls are enabled at the operating system, database, or application level;
2.1.3 administrative access will be restricted to prevent changes to systems or applications;
2.1.4 users will be assigned a single account and prohibited from sharing accounts.

3. Access control to devices and laptops

3.1 Service Provider will implement and maintain commercially reasonable security measures with respect mobile devices and laptops that are used to Process Personal Data.

4. Access control to Personal Data

4.1 Access will be granted only after Processing an approved "access control form", i.e. LAN Logon ID, application access ID, or other similar identification.
4.2 Unique User IDs and passwords will be issued to the users.
4.3 Users, once authenticated, will be authorized for access levels based on their job functions.

5. Transmission and disclosure control

5.1 Service Provider will implement and maintain measures to prevent that Personal Data can be read, copied, modified or removed without authorization during electronic transmission or transport, and to enable to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.
5.2 Service Provider will maintain reasonable technology and processes designed to minimize access for illegitimate Processing, including technology for the encryption of Personal Data.

6. Input control

6.1 Service Provider will maintain system and database logs for access to all Personal Data under its control;
6.2 All Service Provider systems relevant to the security of Personal Data must be configured to provide event logging to identify a system compromise, unauthorized access, or any other security violation. Logs must be protected from unauthorized access or modification;
6.3 Service Provider will maintain input controls on its systems as relevant to the security of Personal Data.

7. Job control

7.1 Service Provider will implement reasonable procedures to ensure the reliability of its employees and any other person acting under its supervision that may come into contact with, or otherwise have access to and Process, those Personal Data, such as requiring a Certificate of Good Conduct ("*VOG*") prior to commencement of employment.
7.2 Service Provider will implement reasonable procedures to ensure that its personnel is aware of its responsibilities under the Agreement. Service Provider shall instruct and train all any persons it authorizes to have access to the Personal Data on the Data Protection Legislation as well as on all relevant security standards and shall commit them in written form to comply with the data secrecy, the Data Protection Legislation and other relevant security standards.
7.3 Service Provider will promptly act to revoke access to Personal Data of relevant employees or contractors of Service Provider due to termination, a change in job function, or in observance of user inactivity or extended absence.
7.4 Service Provider shall have in place a data protection policy and a document retention policy, with which its personnel must comply.

8 Incident management

8.1 Service Provider will implement, maintain an incident management procedure that allows Service Provider to inform the Controller within the required time frame of any security breach.
8.2. May a security breach (potentially) affect personal data, Service Provider must notify Randstad as per provision 4 in the Addendum.
8.3 The incident management procedure include periodic evaluation of recurring issues that might indicate a security breach.

9. Availability control

9.1 Service Provider will use all commercially reasonable endeavours to protect Personal Data against accidental destruction or loss by ensuring:
9.1.1 Workstations that are used to Process Personal Data will be protected by commercial anti-virus and malware prevention software receiving regular definition updates;
9.1.2 Upon detection of a virus or malware, Service Provider will take immediate reasonable steps to arrest the spread and damage of the virus or malware and to eradicate the virus or malware.

10. Business continuity management

10.1 Service Provider will implement, maintain a business continuity plan.
10.2 Service Provider will regularly evaluate this plan.

11. Change management

11.1 Service Provider will implement, maintain a change management procedure.
11.2 As part of the change management procedure Service Provider will evaluate the impact on the security and adapt the measures where needed to maintain the agreed security level.