Data Processing Agreement

This Data Processing Agreement (the "**Agreement**") will become effective as at the date the following parties have validly completed and executed it:

(1) **Checking Your Staff Limited**, with **Company No. 14966634**, whose registered office is at **Premier House, Bradford Road, Cleckheaton BD19 3TT** ("**Vendor**"); and

(Client) , a company incorporated in England, with corporate number **( )** and having its registered office at ( ) ("**Customer**").
Vendor and Customer are hereinafter collectively referred to as "the Parties" or each individually as a "Party".

WHEREAS:

(A) Vendor and Customer have entered into written services agreements or any other relevant agreements (the "Principal Agreements")(APPENDIX 1) which involve Processing (as defined in Clause 1.10 below) of Personal Data (as defined in Clause 1.7 below) of Data Subjects (as defined in Clause
1.3 below) subject to EU Data Protection Law (as defined in Clause 1.4 below) for in the context of the Services provided in the Principal Agreements.

(B) The Parties have agreed to enter into a data processing agreement which shall govern the Processing of Personal Data of Data Subjects subject to EU Data Protection Law in the context of the Services provided in the Principal Agreements. (APPENDIX 1)

NOW, THEREFORE, the Parties agree as follows:

A. This Agreement regulates the Processing of Personal Data of Data Subjects subject to EU Data Protection Law for the Purposes (as defined in Appendix 1 below) by the Parties in the context of the Services provided in Appendix 1.

B. By signing the Agreement, Customer enters into this Agreement on behalf of itself and, to the extent required under EU Data Protection Law, in the name and on behalf of its Affiliates (as defined in Clause 1.1 below), if and to the extent Vendor and/or any of its Affiliates Processes Personal Data for which such Customer Affiliates qualify as the Controller.

C. For the purposes of this Agreement only, and except where indicated otherwise, the term "Customer" shall include Customer and Customer's Affiliates listed in Schedule 1 and "Vendor" shall include Vendor and Vendor's Affiliates listed in Schedule 2.

D. The Parties agree that the terms as set out below supersede and replace any existing privacy and data protection terms contained in the Principal Agreements pertaining to the Processing of Personal Data subject to EU Data Protection Law.

Following Appendices form an integral part of this Agreement:

- APPENDIX 1: Checking Your Staff Principal Service Agreement
- APPENDIX 2: Description of the processing Activities
- APPENDIX 3: List of Security Measures

1. Definitions. The following terms have the meanings set out below for this Agreement:

1.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. “Controller” means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

1.3. “Data Subject” means the natural person whose Personal Data are processed in the context of the Agreement.

1.4. “EU Data Protection Law” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

1.5. “Europe” means the EEA, Switzerland, Monaco and the United Kingdom.

1.6. “GDPR” means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).

1.7. “Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.8. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.9. “Processor” means the entity which processes Personal Data on behalf of a Controller.

1.10. “Processing of Personal Data” (or “Processing/Process”) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11. “Sensitive Data” means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any future revision of EU Data Protection Law.

1.12. “Sub-Processor” means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

2. **Roles of the Parties.** For the purpose of the Agreement, the Parties acknowledge and confirm that:

2.1. Customer is the Controller and Vendor acts as the Processor for the Processing of Personal Data for the Purposes (as defined in Appendix 1) in the context of the Services and in compliance with EU Data Protection Law.

3. **Obligations of Customer.** Customer represents and warrants that, in relation to the Processing of Personal Data for the Purposes in the context of the Services, it acts as a Controller and that it:

3.1. Complies with EU Data Protection Law in respect of Processing of Personal Data, and only gives lawful instructions to Vendor (Lawfulness of processing).

3.2. Relies on a valid legal ground under EU Data Protection Law for each Purpose, including obtaining Data Subjects' appropriate consent if required or appropriate under EU Data Protection Law (Legal ground).

3.3. Provides appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data for the Purposes, in a timely manner and at the minimum with the elements required under EU Data Protection Law, (2) the existence of Processors located outside of Europe; (1) the transfer of any Sensitive Data prior to transferring them to a country that does not provide an adequate level of protection (Notice).

3.4. Takes reasonable steps to ensure that Personal Data is accurate, complete and current; adequate, relevant and limited to what is necessary in relation to the Purposes for which they are processed; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the Purposes for which the Personal Data are processed unless a longer retention is required or allowed under applicable law (Accuracy, data minimization and data retention).

3.5. Implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law, including, as appropriate, appointing a data protection officer, maintaining records of processing, complying with the principles of data protection by design and by default and, where required, performing data protection impact assessments and conducting prior consultations with supervisory authorities (Accountability).

3.6. Responds to Data Subject requests to exercise their rights of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing in accordance with EU Data Protection Law (Data Subjects' Rights).

3.7. Cooperates with Vendor to fulfil their respective data protection compliance obligations in accordance with EU Data Protection Law (Cooperation).

4. **Obligations of Vendor.** Vendor will comply with EU Data Protection Law when Processing Personal Data for the Purposes in connection with the Services, and it will:

4.1. Only Process Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in Appendix 1, Clause 2, or as otherwise agreed by both Parties in writing.

4.2. Promptly inform Customer if, in its opinion, the Customer's instructions infringe EU Data Protection Law, or if Vendor is unable to comply with the Customers' instructions.

4.3. Cooperate with Customer in its role as Controller to fulfil its own data protection compliance obligations under EU Data Protection Law, including by providing all information available to Vendor as necessary to demonstrate compliance with the Customer's own obligations and where applicable to help Customer conducting data protection impact assessments or prior consultation with supervisory authorities.

4.4. Keep internal records of Processing of Personal Data carried out as a Processor on behalf of Customer.

4.5. Assist Customer in fulfilling its obligation to respond to Data Subjects' requests to exercise their rights as provided under EU Data Protection Law and specified under Clause 3.6., and notify Customer about such requests if Vendor receives it directly from the Data Subject.

4.6. Notify Customer when local laws prevent Vendor (1) from fulfilling its obligations under this Agreement and have a substantial adverse effect on the guarantees provided by this Agreement, and (2) from complying with the instructions received from the Customer via the Agreement, except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

4.7. When the Agreement expires or upon termination of the Agreement or upon a request to delete or return Personal Data by Customer, except for any Personal Data which Vendor Processes as a Controller, Vendor will, at the choice of Customer, delete, anonymize, or return such Personal Data to Customer, and delete or anonymize existing copies unless applicable law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case Vendor will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore).

5. **Data Transfers**. Customer authorizes Vendor to transfer the Personal Data Processed in connection with the Services outside of Europe in accordance with any other lawful data transfer mechanism that provides an adequate level of protection under EU Data Protection Law. Vendor represents and warrants that it will abide by EU Data Protection Law when Processing Personal Data for the Purposes in the context of the Services.

6. **Sub-Processing.** Customer gives a general authorization to Vendor to process and sub- process Personal Data to internal and external Sub-Processors in the context of the Services under the conditions set forth below and Vendor represents and warrants that when sub-processing the Processing of Personal Data in the context of the Services, it:

6.1. Requires its external Sub-Processors, via a written agreement, to comply with the requirements of EU Data Protection Law applicable to processors and data transfers, with the Customer's instructions and with the same obligations as are imposed on Vendor by the agreement.

6.2. Remains liable to the Customer for the performance of its Sub-Processors' obligations.

6.3. Commits to provide a list of Sub-Processors to Customer upon request.

6.4. Will inform Customer of any addition or replacement of a Sub-Processor in a timely fashion so as to give Customer an opportunity to object to the change or to terminate the Agreement before the Personal Data is communicated to the new Sub-Processor, except where the Services cannot be provided without the involvement of a specific Sub-processor.

7. SECURITY OF THE PROCESSING; CONFIDENTIALITY; AND PERSONAL DATA BREACH.

7.1. The Parties must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Appendix 2 and as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. In assessing the appropriate level of security, the Parties must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Security measures).

7.2. The Parties must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and if applicable Process Personal Data in accordance with the Controller's instructions (Confidentiality).

7.3. The Parties must notify a Personal Data Breach that relates to Personal Data Processed in the context of the Service to the other Party, without undue delay, and no later than 48 hours after having become aware of a Personal Data Breach. Vendor will provide reasonable assistance to Customer in complying with its obligations to notify a Personal Data Breach. (Personal Data Breaches).

7.4. The Parties will use their best efforts to reach an agreement on whether and how to notify a Personal Data Breach, and must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial action taken (Cooperation and Documentation in case of Personal Data Breaches).

8. **Data Protection Audit.** Upon prior written request by Customer, Vendor agrees to cooperate and within reasonable time provide Customer with: (a) a summary of the audit reports demonstrating Vendor's compliance with EU Data Protection obligations under this Agreement, after redacting any confidential and commercially sensitive information; and

(b) confirmation that the audit has not revealed any material vulnerability in Vendor's systems, or to the extent that any such vulnerability was detected, that Vendor has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection law or reveal some material issues, subject to the strictest confidentiality obligations, Vendor allows Customer to request an audit of Vendor's data protection compliance program by external independent auditors, which are jointly selected by the Parties. The external independent auditor cannot be a competitor of Vendor, and the Parties will mutually agree upon the scope, timing, and duration of the audit. Vendor will make available to Customer the result of the audit of its data protection compliance program.

9. **Liability towards Data Subjects.** Subject to the liability clauses in the Principal Agreements, the Parties agree that they will be held liable for violations of EU Data Protection Law towards Data Subjects as follows:

9.1. Customer is responsible for the damage caused by the Processing which infringes EU Data Protection Law or the Agreement.

9.2. When Vendor acts as a Processor, it will be liable for the damage caused by the Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to Processors or where it has acted outside of or contrary to Customer's lawful instructions. In that context, Vendor will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

9.3. Where the Parties are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Customer and Vendor may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Vendor paid full compensation for the damage suffered, it is entitled to claim back from

Customer that part of the compensation corresponding to Customer's part of responsibility for the damage.

10. **Applicable Law and Jurisdiction**. The Processing of Personal Data under this Agreement is governed by English law. Any disputes between the Parties relating to the Processing of Personal Data under this Agreement will be subject to the exclusive jurisdiction of the courts in England.

11. **Modification of this Agreement**. This Agreement may only be modified by a written amendment signed by each of the Parties.

12. **Termination.** The Parties agree that this Agreement is terminated upon the termination of all the Principle Agreements.

13. **Invalidity and Severability.** If any provision of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this Agreement and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

14. **Counterparts**. This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

(signature page follows)

IN WITNESS WHEREOF, Vendor and Customer have executed this Agreement and each acknowledges having received a duly executed copy.

Checking Your Staff Ltd	
Signed:	
Name:	Mr Nicholas Allan
Title:	Owner
Dated:	14/02/24

Client	
Signed:	
Company	
Name:	
Title:	
Dated:	

SCHEDULE 1: LIST OF CUSTOMER AFFILIATES

Not Applicable

SCHEDULE 2: LIST OF VENDOR AFFILIATES

APPENDIX 1: CHECKING YOUR STAFF LIMITED PRINCIPAL SERVICE AGREEMENT

CHECKING YOUR STAFF LIMITED PRINCIPAL SERVICE AGREEMENT

This principal services agreement is made between Checking Your Staff Limited (CYS) of Premier House, Bradord Road, Cleckheaton BD19 3TT on the one part and the company named as the client in the schedule of the other part (the client).

The client wishes CYS to provide compliant candidate vetting and screening services to the client and CYS wishes to provide such services. By signing this you agree to CYS proving these services via its online and hardcopy vetting and screening processes.

Client Details.

As per email communication and original terms agreed and signed.

Services required.

Agreed Payment Terms.

The client shall pay Checking Your Staff Limited at the agreed payment rate as originally set out or as agreed by both parties since and not in any way different.

Checking Your Staff LImited	
Signed:	
Name:	Mr Nicholas Allan
Title:	Owner
Dated:	14/02/2024

Cient	
Signed:	
Company	
Name:	
Title:	
Dated:	

APPENDIX 2: DESCRIPTION OF THE PROCESSING ACTIVITIES

1. SUBJECT-MATTER OF THE PROCESSING

The subject matter of the Processing is set out in the Principal Agreement

2. NATURE AND PURPOSE OF THE PROCESSING

Candidate Vetting and Screening

3. TYPES OF PERSONAL DATA

As per the CYS Privacy Notice

4. CATEGORIES OF DATA SUBJECTS

Employees of the “Data Controller”

5. DURATION OF THE PROCESSING

For the duration necessary for:

Until completion of the vetting and screening requested by the “Data Controller”

APPENDIX 3: SECURITY MEASURES

The Parties will, as a minimum, implement the following types of security measures:

1. PHYSICAL ACCESS CONTROL

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Established security areas.
- Controlled access for employees and visitors.
- Agreed Keyholders
- Key management and key holder logging
- Onsite 24 hour building supervisor.
- Main Access to building locked AM and PM
- Building is alarmed and CCTV in place.
- We have no decentralized data processing equipment and personal computers.

2. VIRTUAL ACCESS CONTROL

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

Our network is secured via a SonicWall and Draytek combination to authenticate users on the network for remote access. The Sonic wall includes a 2 step authentication process to gain access.

All passwords on the network require a minimum 7 letters with Capital letters, Special Characters and numbers for the combination.

All network passwords are set to reset at 30 days.

All desktop machines are set to lock the screen with password log after 5 mins.

The network is continually monitored for security breaches through the log files of the Draytek router and also the SonicWall logs.

The creation of a single user account in Active directory allows us to manage the accounts and creation of master records on the network.

3. DATA ACCESS CONTROL

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such personal data in accordance with their access rights, and that personal data cannot be read, copied, modified or deleted without authorization, include:

All Internal data is held on a central server that is accessed by users logging on to our domain and then the central server this is controlled by the password lockout policy.

External access to the data is controlled via VPN and also Active Directory security.

Database access is granted through a strict username and password policy to allow access to certain areas of the data.

The policies in place allow different access levels and security restrictions.

All data and access requests for data on the network is logged and reviewed on a weekly basis

Access to the network is created only to Bextec Limited. No other organizations have access to the network to ensure that we can strictly control data access and distribution.

Email servers have extended TLS security to ensure that the certification and security of emails in and out of the organization are secure at all times.

A monthly review of server security and patching takes place every month to ensure that all security patches are applied and also all security breach attempts are recorded, covered and closed.

All data that is not useful is securely removed using Blannco date destruction software.

4. DISCLOSURE CONTROL

Technical and organizational measures to ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities personal data are disclosed, include:

All communication to the email servers and data servers are controlled through SSL certificates and L2TP security protocols to ensure data transmitted is secure and authenticated.

Our VPN is controlled via L2TP protocols, to ensure that all data is authenticated.

SSL certificates are in place to secure the transmission of data. ALL certificates are set to 2048 bit encryption.

5. ENTRY CONTROL

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

All systems are updated and patched on a monthly basis to ensure that all security patches are applied.

To ensure that all systems are operating correctly and not transmitting any data that they shouldn't.

All systems require an administrative account access to install or create any systems changes.

All system updates and patches are recorded when these updates take place.

6. CONTROL OF INSTRUCTIONS

Technical and organizational measures to ensure that personal data are processed solely in accordance with the instructions of the controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. AVAILABILITY CONTROL

Technical and organizational measures to ensure that personal data are protected against accidental destruction or loss (physical/logical) include:

Full backup of Sql server, Exchange server, every 24 hours ensuring all changes are tracked and recoverable. 1 week of backups are held on the Azure cloud in Northern Europe.

ALL servers run from Mirrored hard drives on a raid mirror.

All systems are run from a UPS which gives 30 minutes power and allows for safe shut down of the systems in the event of power loss.

All systems run McAfee enterprise antivirus. This will shortly be upgraded to Vipre.

The whole network is secured from Behind the SonicWall Firewall.

In the event of a disaster, we can recover to within 24 hours of data.

8. SEPARATION CONTROL

Technical and organizational measures to ensure that personal data collected for different purposes can be processed separately include: