UK Standard Contractual Clauses

Name of the data exporting organisation: Customer as identified in the online order form or the Workable Quote as applicable

Address: Customer's address as identified in the online order form or the Workable Quote as applicable

Tel: N/A fax: N/A; e-mail: N/A

Other information needed to identify the organisation

[***insert***]

(the data **exporter**)

And

Name of the data importing organisation: Workable Software Ltd

Address: 5 Golden Square, 5th Floor, London W1F 9BS, United Kingdom

Tel: [*insert*]; fax: N/A; e-mail: [*insert*]

Other information needed to identify the organisation

Registered in England and Wales with Company Registration number 08125469

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1 Definitions

For the purposes of the Clauses:

(a) '**personal data**', '**special categories of data**', '**process/processing** ', '**controller** ', '**processor**', '**data subject**' and ' **supervisory authority**' shall have the same meaning as in the UK GDPR

(b) '**the data exporter**' means the controller who transfers the personal data;

(c) '**the data importer**' means the processor who agrees to receive from the data

exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses

and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act ;

(d) '**the sub-processor**' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '**the applicable data protection law**' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) '**technical and organisational security measures**' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2 Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3 Third-party beneficiary clause

1.The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the

data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4 Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act ;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

5 Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a

prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter
and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6 Liability

1.The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2.If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3.If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

7 Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by Commissioner.

(b) to refer the dispute to the UK courts.

2. The parties agree that the choice made by the data subject will not prejudice its

substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8 Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9 Governing law

The Clauses shall be governed by the country of the United Kingdom in which the data exporter is established,

10 Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11 Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor

entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law country of the UK where the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner.

12 Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data importer is (please specify briefly activities relevant to the transfer):
Applicant Tracking System

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees, including current and former employees, trainees and interns, pre-hires, applicants and sourced candidates.

External recruitment consultants

Categories of data

The personal data transferred concern the following categories of data (please specify):

Name (name and surname)

Address

Nationality

Password

User name

E-mail address

Telephone number

Salary

Employment terms (incl salary and benefits)

IP-address

Links to social profiles
Resume

The Controller may choose to store additional information on candidates.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Processor does not anticipate processing any data falling into the special categories of data as set out in the UK GDPR, however, it is not possible for Processor to control the information that candidates or authorized users of the Controller choose to share with each other using the Service.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Collection

Registration

Storing

Accessing, reading or consultation

Erasure or destruction

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Technical and Organizational Security Measure	**Details**
Measures of pseudonymisation and encryption of personal data	All Application data - including personal data such as candidates information - is always encrypted at-rest and in-transit in order to ensure its confidentiality across all its lifecycle (e.g.: storage means, data flows). Personal data is stored on a microservice level to apply segregation and segmentation across the Application storage resources(e.g.: databases). Randomly generated and long UUIDs are used to correlate data to an individual.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Workable data is encrypted at rest and in transit using Security Best Practices and the latest recommended secure cipher suites and protocols Appropriate safeguards have been implemented to protect the creation, storage, retrieval and destruction of secrets. Workable implements Best Practices as they evolve and respond promptly to cryptographic weaknesses as they are discovered.

	The infrastructure and data are stored redundantly in multiple locations in their hosting and data storage providers. Workable uses multiple relational databases for its applications. Each database server has an independent synchronous replica in a different availability zone within the same AWS region to mitigate the risk of data lost due to hardware failure. In the unlikely event of a major disaster, a Business Continuity Plan (BCP) is in place to help guarantee a smooth and organized transition towards a full recovery. To ensure that production services are highly available, teams have designed infrastructure so as to have replicas/ fallbacks for all critical resources. To ensure that Workable infrastructure is resilient against single node or instance failure, for all critical services multiple instances are available and running. This guarantees that if a single instance fails there is at least an extra instance to serve traffic until the failure is recovered. In order to protect services from single zone failure of cloud providers, all critical resources have multi-zone availability. This means that when teams provision production resources they make sure that they have replicas in multiple zones, so if a single zone fails the replicas in the other zones can still serve traffic
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Workable has documented and follows specific policies and procedures to securely take, maintain, test and restore backups of production data. Backup data includes but is not limited to customers' and candidates' data, application logs and systems' configuration, and has a retention period of at least 18 months. The backup configuration of a new resource is not limited to availability factors (e.g.: retention period, frequency) but also includes restoration aspects such as integrity tests and restore periodic procedure and timeline.. The enterprise cloud platforms (e.g.: GCP and AWS), where Workable infrastructure is hosted, offer strong and out of the box managed backup services ensuring data availability and integrity.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Workable has identified a suitable, systematic approach and framework for risk assessment which is appropriate for its business, legal, regulatory and contractual requirements, and this is described in the Risk Assessment Report. Assessment (analysis and evaluation) of risks is

	carried out at least once a year, options for risk treatment are identified and evaluated in line with the Risk Assessment process. Technical security assessments (such as web application penetration testing, manual source code review and configuration audit) are performed by 3rd-party security experts on a regular basis to bring independent expertise and in-depth testing.. The ISMS is thoroughly reviewed through an Audit Program maintained by the CISO. The goal of internal and external audits is to: • Identify potential non-compliance points with respect to Workable policies, procedures as well as regulatory requirements (e.g.: GDPR, CCPA, etc.) and Standards (e.g.: ISO 27001, ISO 27017, AICPA TSC.) • Spot opportunity for improvements • Document and track remediation activities All appropriate mitigation actions such as technical security assessments and audit findings are documented, reviewed, approved and tracked for their effective implementation.
Measures for user identification and authorization	As a Product: • The Workable application ensures a strong authentication flow with hardened configuration (e.g.: password policy, account lockout, Captcha mechanism) and secure protocols including SAML v2 and OIDC. • Appropriate Logical Access controls and restrictions are in place on the account and user level of the application while the customer can enforce a granular authorization model based on the different available user roles. As a Company: • Workable systems and services use strong authentication means (such as SSO, TFA and short session timeouts). Credentials are managed through an enterprise cloud vault solution ensuring password complexity and prohibiting password reuse. • Granular role-based access control is in place for all Workable employees based on their position and need to know principle. Access is managed via a dedicated procedure while an entitlement review process is performed during the internal audits.

Measures for the protection of data during transmission	Data is always encrypted in-transit to ensure its confidentiality using Security Best Practices and the latest recommended secure cipher suites and protocols.
Measures for the protection of data during storage	Data is always encrypted at-rest to ensure its confidentiality and integrity using Security Best Practices and the latest recommended secure cipher suites and protocols. On top of all cloud storage resources, Workable laptops and mobile devices are fully encrypted.
Measures for ensuring physical security of locations at which personal data are processed	Offices: • Access to the premises is protected by physical access controls such as security guards, access cards, CCTV and alarm system.Guest and external visitors' access is handled securely through a dedicated procedure. Cloud resources: • Workable uses subservice organizations (Google Cloud Platform and Amazon Web Services) for cloud hosting services and for providing physical controls, environmental controls, infrastructure support and storage services. Workable reviews the reports and/ or certifications (e.g. SOC 2, ISO) of the subservice contractors in regard to security controls including data centers physical and environmental controls
Measures for ensuring events logging	Workable maintains an extensive, centralized logging system in the production environment. It contains information pertaining to security, monitoring, availability and access, as well as other metrics about our application ecosystem and its microservices. Production log retention is set to 18 months. These logs are analyzed for security events and abnormalities via logical and technical controls. Further, alerts and monitors automatically notify appropriate internal teams 24/7/365 to ensure visibility and responsiveness. These alerts also include the product availability, capacity and performance metrics. Production operation actions (such as major system configuration update and product deployments) are performed in a controlled (segregated responsibilities, approval step) and tracked (audit logs) manner.
Measures for ensuring system configuration, including default configuration	Security best practices are taken into account during the installation of any resource in the cloud infrastructure in order to ensure that cloud

	infrastructure complies with Workable Security Policies. A production readiness checklist depicts the high level controls (e.g.: access controls requirements, encryption, patch management, backup strategy, logging requirements, etc.) that have to be met for all production systems. Each control is detailed for each type of resource (e.g.: vm, database).
Measures for internal IT and IT security governance and management	Workable maintains reasonable and appropriate technical and organizational controls (based on best practices, i.e. ISO 27001, ISO 27017 and SOC 2 requirements) in order to protect customer data against accidental loss, destruction or alteration, unauthorized disclosure or unlawful destruction. Workable compliance requirements are continuously monitored and reviewed and appropriate changes to Information Security Policies and technical controls are performed as needed. The Legal Department and DPO are responsible to ensure that all requirements from applicable legislation are communicated to the Security department. The Security Department is responsible to review the policies and procedures in order to achieve compliance with the regulatory requirements Workable undertakes management review of the ISMS on a regular basis (are held at not greater than six-monthly intervals) to ensure that the scope remains adequate and improvements in the ISMS process are identified. The agenda of Management Review Meetings covers all the items that are required by the relative standards (i.e. ISO 27001:2013, ISO 27017:2015, AICPA Trust Services Criteria, etc.). All actions that are decided during the management review meeting are monitored in order to ensure their implementation and effectiveness
Measures for certification/assurance of processes and products	Workable holds security certifications and comply with industry-accepted standards and regulations: • ISO 27001:2013, Information Security Management System • ISO 27017:2015, Security Controls for the Provision and Use of Cloud Services • SOC 2 Type I report Additionally, Technical Security Assessments (such as web application penetration testing,

	manual source code review, configuration audit, etc.) are performed by 3rd-party security experts on a regular basis.
Measures for ensuring data minimisation	In compliance with the GDPR / CCPA requirement, the Workable product provides its customers the ability to have control over their data. Data deletion requests are handled through a dedicated automated process. The Application enforces controls on all upload flows to ensure that only the allowed file types are stored within the system. Moreover, the terms of use clearly state the types of information that should be stored within Workable as well as the customers' responsibility regarding its use.
Measures for ensuring data quality	Users' input is sanitized and validated by the application in regards to the business logic of the corresponding feature or product. Malformed data is thus rejected prior to be stored.
Measures for ensuring limited data retention	Workable Customers determine what Customer Data they process via Workable product. As such, Workable operates on a shared responsibility model. If a Customer is unable to delete Customer Data via the self-services functionality of the Product, then Workable deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.
Measures for ensuring accountability	Management has defined Roles and Responsibilities to oversee implementation of the Information Security Policy across Workable (e.g. DPO has been appointed, Information Security Committee is in place as well as specific security responsibilities for Workable Team Members). New employees undergo initial training during the onboarding week to understand their key responsibilities, tasks and Team's process. The Employment Agreement and the Acceptable Use Policy are signed by the end of the first week. Employees are evaluated on a periodic basis based on their role specific goals and overall performance. Regular meetings on SVPs / VPs level as well as Management Review Meetings (MRMs) are conducted regarding information security. The topics of these meetings include results from risk assessments, internal and external audits, security assessments,other feedback from interested parties and appropriate corrective and preventive decisions are taken. Major gaps are communicated to the

	Board of Directors through Management Review Meetings (MRMs). Internal & external information security audits are performed at least on an annual basis in order to ensure compliance with Data Protection (e.g. GDPR, CCPA) and Information Security requirements (e.g. Workable policies & procedures, ISO 27001, ISO 27017, TSC, Security Best Practices). All identified gaps are investigated, and appropriate corrective and preventive actions are implemented via formal procedures. Major gaps are communicated to the Board of Directors through Management Review Meetings (MRMs).
Measures for allowing data portability and ensuring erasure	As a Product: • Workable provides the appropriate tools that give Customer control over their data, ensuring compliance with GDPR / CCPA requirements. Additionally, appropriate operation procedures are in place internally in order to handle GDPR / CCPA requests in case Customer is not able to handle any data subject request. As a Company: • When a critical tool or service is sunsetted, Workable asks for confirmation in writing regarding permanent data deletion. • Physical devices such as laptops and hard drives are wiped according to the device disposal policy.
Technical and organizational measures of sub-processors	Third parties and contractors Non-Disclosure Agreements (NDA), Data Processing Agreements (DPA) and contracts are in place and contain provisions in regard to confidentiality clauses and code of conduct if applicable. In particular Workable enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this Agreement. Each sub-processor agreement must ensure that Workable is able to meet its obligations to the Customer and technical and organisational measures shall be implemented in order to safeguard the protection of personal data. Sub-processors must without limitation a) notify Workable in the event of a Security Incident without undue delay so Workable may notify Customer accordingly; b) delete data when instructed by Workable in accordance with Customer's instructions to Workable; c) not engage additional sub-processors without authorization; d) not change the location where data is processed; or

	e) process data in a manner which conflicts with Customer's instructions to Workable. e) enter into a separate agreement containing the applicable SCCs, when this is required. Appropriate contracts and Service Level Agreements (SLAs) are in place to outline and communicate the terms, conditions and responsibilities for third-party providers. (e.g. Google Cloud, Amazon).