STANDARD CONTRACTUAL CLAUSES

Module 2

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(*omitted*)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall

have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause
12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause
13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause
14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic

society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause
15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause

16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Greece.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Greece.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I

1. **LIST OF PARTIES**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: 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

Contact person's name, position and contact details:

Signature and date: The date of execution of the Quote

Role (controller/processor): Controller

Data importer(s): Name: The Workable entity identified in the online terms or the Workable Quote as applicable

Address: The address identified in the online terms or the Workable Quote as applicable

Contact person's name, position and contact details: support@workable.com

Activities relevant to the data transferred under these Clauses: ATS service provider

Signature and date: The date of execution of the Quote

Role (controller/processor): Processor

2. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

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 personal data transferred

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

Name (name and surname)

Address

Nationality

Password

Username

E-mail address

Telephone number

Salary

Employment terms (incl salary and benefits)

IP-address

Links to social profiles

Resume

Videos

The Exporter may choose to store additional information on candidates.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

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

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer is a continuous basis for the duration of the Services as identified in the Workable Quote.

Nature of the processing

The Importer will process and access personal data on a routinely basis as necessary to provide the Services as described in the Workable Terms.

The below processing activities take place:

Collection

Registration

Storing

Accessing, reading or consultation

Erasure or destruction

Purpose(s) of the data transfer and further processing

The Importer will process Personal Data as necessary to provide the Services under the Workable Terms.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The Importer will process Personal Data for the purpose of providing the Services for the duration of the Services as identified in the Quote or until the Exporter elects to delete such Personal Data via the Workable Platform. In relation to storage of the Personal Data, the Processing shall cease in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The transfer to sub-processors is on continuous basis for the duration of the Services.

3. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Hellenic Data Protection Authority

4. LIST OF AUTHORISED SUBPROCESSORS

The Exporter has authorized the use of the sub-processors identified at:

https://www.workable.com/subprocessors

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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 • SOC 2 Type II Report • SOC 3 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).