compete

COMPETE
- DATA PROCESSING ADDENDUM -

Updated: 1/8/2022

This Data Processing Addendum ("**DPA**") forms an integral part of the commercial agreement or any other agreement ("**Agreement**") in connection with the provision of services by and between Compete HR Ltd. ("**Compete**"), the provider of services under the Agreement (the "**Services**"), and the recipient of services under the Agreement ("**Customer**"), to reflect the parties' agreement on the Processing of Customer Personal Data.

All capitalized terms not defined herein will have the meaning set forth in the Agreement, or under applicable Privacy Laws and Regulations. All terms under the Agreement apply to this DPA, except that the terms of this DPA will supersede any conflicting terms under the Agreement.

In the course of providing the Services, Compete may Process Customer Personal Data. Accordingly, the parties agree to comply with the following provisions under this DPA with respect to the Processing of Customer Personal Data, as further described herein.

1. DEFINITIONS

1.1. "**Customer Personal Data**" means Personal Data Processed by Compete on behalf of Customer as part of the provision of Services.

1.2. "**Data Subject**" means 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.

1.3. "**EU SCCs**" means the Standard Contractual Clauses pursuant to EU Commission Decision C(2021)3972, available here.

1.4. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise processed.

1.5. "**Personnel**" means persons authorized by Compete to Process Customer Personal Data.

1.6. "**Privacy Laws and Regulations**" means 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 and repealing Directive 95/46/EC ("**GDPR**"), and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**").

1.7. "**Third Country**" means a country outside the European Economic Area or the UK which was not acknowledged by the EU Commission or a UK Secretary of State as providing an adequate level of protection in accordance with Article 45(3) of the GDPR or Article 45 of the UK GDPR.

2. DATA PROCESSING

2.1. **Scope and Roles**. This DPA applies when Customer Personal Data is Processed by Compete as part of Compete's provision of the Services, as further specified in the Agreement and the applicable order form. In this context, to the extent that provisions under Privacy Laws and Regulations apply to Customer Personal Data, Customer is the Controller and Compete is the Processor.

2.2. **Subject Matter, Duration, Nature, and Purpose of Processing**. Compete processes Customer Personal Data as part of providing Customer with the Services, pursuant to the specifications and for the duration under the terms of the Agreement.

2.3. **Instructions for Compete's Processing of Customer Personal Data**. Compete will only Process Customer Personal Data on behalf of and in accordance with Customer's instructions. Customer instructs Compete to Process Customer Personal Data for the following purposes:

2.3.1. Processing in accordance with the Agreement and applicable order forms, including, without limitation to provide, operate, control, supervise, and safeguard the Services – all integral parts of the provision of the Services to Customer;

2.3.2. Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement and comply with applicable Privacy Laws and Regulations. Processing outside the scope of this DPA (if any) will require prior written agreement between Compete and Customer on additional instructions for Processing, including agreement on any additional fees Customer will pay to Compete for carrying out such instructions.

2.4. As required under applicable Privacy Laws and Regulations, Compete will inform Customer immediately, if in Compete's opinion an instruction violates any provision under applicable Privacy Laws and Regulations and will be under no obligation to follow such instruction, until the matter is resolved following a good-faith discussion between the parties.

2.5. Compete will not retain, use, or disclose Customer Personal Data: (A) for any purpose other than for the specific purpose of performing the Services, or (B) outside of the direct business relationship between Customer and Compete, except as permitted under applicable Privacy Laws and Regulations. Compete acknowledges and will comply with the restrictions set forth in this Section 2.5.

2.6. Customer undertakes to provide all necessary notices to Individuals and receive all necessary permissions and consents, or otherwise secure the required lawful ground of Processing, as necessary for Compete to process Personal Data under the terms of the Agreement and this DPA, pursuant to applicable Privacy Laws and Regulations, including with respect to the cross-border of Personal Data.

2.7. To the extent required under applicable Privacy Laws And Regulations, Customer will appropriately document the Individuals' notices and consents, or necessary assessment with other applicable lawful grounds of Processing.

3. ASSISTANCE

Taking into account the nature of the Processing, Compete will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising Data Subjects' rights, as required under applicable Privacy Laws and Regulations. Compete will further assist Customer in ensuring compliance with Customer's obligations in connection with the security of Processing, notification of a Personal Data Breach to supervisory authorities and affected Data Subjects, Customer's data protection impact assessments and Customer's prior consultation with supervisory authorities, in relation to Compete's Processing of Customer Personal Data under this DPA. Except for negligible costs, Customer will reimburse Compete with costs and expenses incurred by Compete in connection with the provision of assistance to Customer under this DPA.

4. COMPETE PERSONNEL

4.1. **Limitation of Access**. Compete will ensure that Compete's access to Customer Personal Data is limited to those personnel who require such access to perform the Agreement.

4.2. **Confidentiality**. Compete will impose appropriate contractual obligations upon Compete Personnel, including relevant obligations regarding confidentiality, data protection, and data security. Compete will ensure that Compete Personnel are informed of the confidential nature of Customer Personal Data, have received appropriate training in their responsibilities, and have executed written confidentiality agreements that bind them by substantially the same material obligations as under this DPA. Compete will ensure that such confidentiality agreements survive the termination of the employment or engagement of its personnel.

5. OTHER PROCESSORS

5.1. Compete may engage third-party service providers to process Customer Personal Data ("**Other Processors**"). Customer hereby provides Compete with a general authorization to engage all Other Processors listed here. All Other Processors have entered into written agreements with Compete that bind them by substantially the same material obligations as under this DPA.

5.2. Compete may engage with a new Other Processor ("**New Processor**") to Process Customer Personal Data on Customer's behalf. Compete will notify Customer of the intended engagement with the New Processor ten (10) days prior to such engagement. Customer may object to the Processing of Customer Personal Data by the New Processor, for reasonable and explained grounds, within five (5) business days following Compete's written notice to Customer of the intended engagement with the New Processor. If Customer timely sends Compete a written objection notice, the parties will make a good-faith effort to resolve Customer's objection. In the absence of a resolution, Compete will make commercially reasonable efforts to provide Customer with the same level of service, without using the New Processor to Process Customer Personal Data.

5.3. **Liability**. Compete will be liable for the acts and omissions related to the Processing of Personal Data by its Other Processors to the same extent that Compete would be liable if performing the Service of each Processor, under the terms of the Agreement.

6. ONWARD AND TRANS-BORDER TRANSFER

6.1. Transfer of GDPR-governed Customer Personal Data ("**EEA Transferred Data**") to a Third Country, is made in accordance with the EU SCCs, giving effect to module three, which is incorporated by reference to this DPA, or as required, in accordance with any successor thereof or an alternative lawful data transfer mechanism, and as follows:

6.1.1. In Clause 7, the optional docking clause will apply;

6.1.2. in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be as set out in Section 5 of this DPA;

6.1.3. In Clause 11, the optional language will not apply;

6.1.4. In Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

6.1.5. In clause 18(b), disputes will be resolved before the courts of Ireland.

6.1.6. Annexes I and II of the EU SCCs will be completed with the relevant information set out in Annexes I and II to this DPA.

6.2. Transfer of UK GDPR-governed Customer Personal Data ("**UK Transferred Data**", and together with EEA Transferred Data: "**Transferred Data**") to a Third Country, is either:

6.2.1. made in accordance with the International Data Transfer Agreement ("**IDTA**"), issued by the Information Commissioner's Office's ("**ICO**") in accordance with section 119A of the Data Protection Act 2018, as officially published here, which is incorporated by reference to this DPA;

or -

6.2.2. made in accordance with the UK Addendum issued by the ICO in accordance with section 119A(1) of the Data Protection Act 2018 (“**UK Addendum**”), incorporating the EU SCCs, as officially published here, which is incorporated by reference to this DPA;

or -

6.2.3. if neither Section 6.3.1 and 6.3.2 apply, then the parties will cooperate in good faith to implement appropriate safeguards for transfers of UK Transferred Data, as required or permitted by the UK GDPR without undue delay.

6.3. In accordance with Article 46 of the GDPR and the EU SCCs, and without prejudice to any provisions of this DPA, Compete undertakes to implement the following organizational and technical safeguards, in addition to the safeguards mandated by the EU SCCs and in accordance with Clause 14(b)(C) of the EU SCCs, to ensure the required adequate level of protection to Transferred Data:

6.3.1. Compete will implement and maintain the technical measures, as specified in Annex II to this DPA, which is attached and incorporated by reference to this DPA, with a purpose to protect the Transferred Data from Processing for national security or other governmental purposes that goes beyond what is necessary and proportionate in a democratic society, considering the type of Processing activities under the Agreement and relevant circumstances;

6.3.2. For the purposes of safeguarding Transferred Data, when any Third Country’s government or regulatory agency requests access to such data (“**Request**”), and unless required by a valid court order or if otherwise Compete may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to Transferred Data, or where the access is requested in the event of imminent threat to lives, Compete will:

6.3.2.1. not purposefully create ‘back doors’ or similar programming that could be used to access Transferred Data;

6.3.2.2. not provide the source code or encryption keys to any government agency for the purpose of accessing Transferred Data; and,

6.3.2.3. upon Customer’s written request, provide reasonable available information about the requests for access to Personal Data by government agencies that Compete has received in the six (6) months preceding to Customer’s request.

6.3.3. If Compete receives a Request, Compete will notify Customer of such request to enable the Customer to take necessary actions, to communicate directly with the relevant agency and to respond to the Request. If Compete is prohibited by law to notify the Customer of the Request, Compete will make reasonable efforts to challenge such prohibition through judicial action or other means at Customer’s expense and, to the extent possible, will provide only the minimum amount of information necessary.

7. INFORMATION SECURITY

Compete will maintain administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of Customer Personal Data. Compete regularly monitors compliance with these safeguards. Compete will not materially decrease the overall security of the Service during the term of the Agreement. Further information about Compete's technical and organizational measures is detailed in **ANNEX II**.

8. AUDIT AND DEMONSTRATION OF COMPLIANCE

Compete will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, in relation to Compete's obligations under this DPA. Compete may satisfy the audit obligation under this section by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors. Other audits by Customer are subject to the following terms: **(A)** the audit will be pre-scheduled in writing with Compete, at least forty-five (45) days in advance and will be performed not more than once a year (unless the audit is required by a Supervisory Authority); **(B)** a third-party auditor will execute a non-disclosure and non-competition undertaking toward Compete; **(C)** the auditor will not have access to non-Customer data **(D)** Customer will make sure that the audit will not interfere with or damage Compete's business activities and information and network systems; **(E)** Customer will bear all costs and expenses related to the audit; **(F)** The auditor will first deliver a draft report to Compete and allow Compete reasonable time and no less than ten (10) business days, to review and respond to the auditor's findings, before submitting the report to the Customer; **(G)** Customer will receive only the auditor's report, with Compete's comments, without any Compete 'raw data' materials, will keep the audit results in strict confidentiality and will use it solely for the specific purposes of the audit under this DPA; and, **(H)** as soon as the purpose of the audit is completed, Customer will permanently and completely dispose of all copies of the audit report.

9. SECURITY BREACH MANAGEMENT AND NOTIFICATION

9.1. Compete maintains security incident management and breach notification policies and procedures and will notify Customer without undue delay after becoming aware of a Personal Data Breach related to Customer Personal Data which Compete, or any of Compete's Other Processors, Process. Compete's notice will at least: **(A)** describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Personal Data records concerned; **(B)** communicate the name and contact details of the Compete's data protection team, which will be available to provide any additional available information about the Personal Data Breach; **(C)** describe the likely consequences of the Personal Data Breach; **(D)** describe the measures taken or proposed to be taken by Compete to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9.2. Compete will work diligently, pursuant to its incident management and breach notification policies and procedures to promptly identify and remediate the cause of the Personal Data Breach and will promptly inform Customer accordingly.

10. DELETION AND RETENTION OF CUSTOMER PERSONAL DATA

10.1. **Data Deletion**. Within reasonable time after the end of the provision of the Service, Compete will return Customer Personal Data to Customer or delete such data, including by de-identifying thereof.

10.2. **Data Retention**. Notwithstanding, Customer acknowledges and agrees that Compete may retain copies of Customer Personal Data as necessary in connection with its routine backup and archiving procedures and to ensure compliance with its legal obligations and its continuing obligations under applicable law, including to retain data pursuant to legal requirements and to use such data to protect Compete, its affiliates, agents, and any person on their behalf in court and administrative proceedings.

11. DISCLOSURE TO COMPETENT AUTHORITIES

Compete may disclose Customer Personal Data: **(A)** if required by a subpoena or other judicial or administrative order, or if otherwise required by law; or **(B)** if Compete deems the disclosure necessary to protect the safety and rights of any person, or the general public.

12. ANONYMIZED AND AGGREGATED DATA

Compete may process data based on extracts of Customer Personal Data on an aggregated and non-identifiable form, for Compete's legitimate business purposes, including for testing, development, controls, and operations of the Services, and may share and retain such data at Compete's discretion, provided that such data cannot reasonably identify a Data Subject.

13. TERM

This DPA will commence on the same date that the Agreement is effective, or as otherwise provided explicitly under this DPA, and will continue until the Agreement expires or is terminated, pursuant to the terms therein.

14. COMPLIANCE

Compete's compliance team is responsible to make sure that all relevant Compete's personnel adhere to this DPA. Compete's compliance team can be reached at: dpo@compete.com

15. DISPUTE RESOLUTION

15.1. Each Party will create an escalation process and provide a written copy to the other Party within five (5) business days of any dispute arising out of or relating to this DPA. The escalation process will be used to address disputed issues related to the performance of this DPA, including but not limited to technical problems. The Parties agree to communicate regularly about any open issues or process problems that require prompt and accurate resolution as set forth in their respective escalation process documentation. The Parties will attempt in good faith to resolve any dispute arising out of or relating to this DPA, before and as a prior condition for commencing legal proceedings of any kind, first as set forth above in the escalation process and next by negotiation between executives who have authority to settle the controversy and who at a higher level of management than the persons with direct responsibility for administration of this DPA.

15.2. Any Party may give the other Party written notice of any dispute not resolved in the normal course of business. Within two (2) business days after delivery of the notice, the receiving Party shall submit to the other a written response. The notice and the response will include: **(A)** a statement of each Party's position and a summary of arguments supporting that position; and, **(B)** the name and title of the executive who will represent that Party and of any other person who will accompany the executive. Within five (5) business days after delivery of the disputing Party's notice, the executives of both Parties shall meet at a mutually acceptable time and place, including telephonically, and thereafter as often as they reasonably deem necessary, to attempt to resolve the dispute. All reasonable requests for information made by one Party to the other will be honored. All negotiations pursuant to this clause are confidential and will be treated as compromise and settlement negotiations for purposes of applicable rules of evidence. The dispute resolution process under this section 15 must be exercised as a pre-condition for initiating legal or administrative proceedings by any of the parties.

16. MISCELLANEOUS

Any alteration or modification of this DPA is not valid unless made in writing and executed by duly authorized personnel of both parties. Invalidation of one or more of the provisions under this DPA will not affect the remaining provisions. Invalid provisions will be replaced to the extent possible by those valid provisions which achieve essentially the same objectives.

ANNEX I
DATA PROCESSING DESCRIPTION

This Annex forms part of the DPA and describes the Processing that the Processor will perform on behalf of the Controller.

A. LIST OF PARTIES

1. **Controller(s) / Data exporter(s)**: Customer whose name, address and contact details are further set out in the Agreement. Customer will provide certain personal data in order to receive the Services pursuant to the Agreement.

2. **Processor(s) / Data importer(s)**: Compete, whose registered name, address and contact details are further set out in the Order Form. Compete will process personal data in order to provide the Services pursuant to the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Customer's employees.
Categories of Customer Personal Data transferred	HR data, for example: legal name, place of employment, department and role, information on employees' terms of employment (e.g., salary, scope, seniority, etc.), gender, age, and nationality, and additional employment related details, as agreed between the parties.
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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures	Financial Information (salary and benefits).
The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)	Continuous.
Nature of the Processing	Provision of Services and associated services.
Purpose(s) of the data transfer and further Processing	As necessary to perform Compete's obligations in accordance with the Agreement.
The period for which the Customer Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	As set out in Clause 10 of the DPA.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the Processing	Same as Above.

C. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter is established in an EU Member State - the supervisory authority of such EU Member State shall act as competent supervisory authority

Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the supervisory authority of the Member State in which the representative is established shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) – the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.

ANNEX II

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

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymization and encryption of personal data	Raw data is encrypted at rest and in transit in accordance with best practices. Data is available to named individuals at Compete for support purposes only and per customer's request.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services	Personal Data is protected against accidental destruction or loss via measures capable of rapidly restoring the availability of and access to Personal Data in the event of a physical or technical incident.
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	Compete holds BCP and DRP programs to ensure integrity, availability, and resilience of processed data (e.g., routine backups, strict access control, periodic recovery testing).
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing	o Backup/recovery testing. o Regular testing of backup system. o Documented process for detecting and reporting security incidents / data breaches (also with regard to mandatory reporting to the relevant supervisory authority \ Data Controllers).
Measures for user identification and authorization	**Technical Measures**: o Access to applications, specifically when entering, changing, and deleting data, is logged. o DLP measures for sensitive files and folders. o Central permission management. o SSH encrypted access. o Certified SSL encryption. **Organizational Measures**: o Use of authorization concepts. o Minimum number of administrators. o Management of user rights by administrators. o Information Security and User Access management Policies.
Measures for the protection of data during transmission	Compete requires TLS 1.3 and enforces HTTPS connection with its servers.
Measures for the protection of data during storage	o All databases are backed up to a dedicated storage bucket and saved for 30 days. o Backup data is encrypted at rest. o Access to backup data is restricted.

Measures for ensuring physical security of locations at which personal data are processed	Compete is a Cloud-native company, with minimal dependency of physical assets. Company devices are 100% mobile. **Technical Measures**: o Employees connect to their systems over a WPA2 secure Wi-Fi connection using company owned and fully managed laptops. o Alarm system. o Automatic access control system. o Smart cards / transponder systems. o Manual locking system. o Doors with knob outside. o Video surveillance of entrances. **Organizational Measures**: o Clean Desk Policy – physical existence of sensitive information is prohibited. o Reception / Receptionist / Gatekeeper. o Employee / visitor badges. o All Visitors are accompanied by employees. o Information Security Policy. o Work instruction access control.
Measures for ensuring events logging	All access to applications is logged, specifically when entering, changing, and deleting data. DLP measures for sensitive files and folders. Security logs are retained for 24 months.
Measures for ensuring system configuration, including default configuration	o Testing and development environments are separated and isolated from the production environment. o Changes are pre-approved by authorized personnel and traced accordingly.
Measures for internal IT and IT security governance and management	Compete holds ISO27001 and ISO27701 certifications.
Measures for certification/assurance of processes and products	o New staff across the company are trained in Secure Software Development Lifecycle (SSDLC) practices. o New product initiatives are reviewed by the security team according to SPbD (Security and Privacy by Design) concepts at the design phase. o System code is tested against known vulnerabilities (e.g., OWASP top 10). o Existing core systems and infrastructure are tested for security vulnerabilities periodically. In some cases, testing is conducted by automatic scanners as well as manually by external independent parties.
Measures for ensuring data minimization	o Collection is limited only to required data to fulfil the specific purpose of the Agreement.

	o Data minimization is assured during our SDLC process.
Measures for ensuring data quality	Data points that have not been updated for 6 months are removed to ensure data accuracy.
Measures for ensuring limited data retention	Duration of the contract. Following termination, Personal Data is deleted or de-identified.
Measures for ensuring accountability	Compete personnel are vetted prior to engagement and are trained periodically with respect to data protection and information security requirements. There are internal policies in place to ensure compliance with privacy laws. Compete is the only authorized entity to process customer personal data.
Measures for allowing data portability and ensuring erasure	Data can be exported from the Compete system by authorized customer's employees.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the Controller and, for transfers from a processor to a sub-processor, to the data exporter.

Measure	Description
[Measures that Compete has in place to assist the Customer in fulfilling its obligations to respond to Data Subject's requests]	Responding to DSARs is at the customer's level.