GDPR Data Processing Addendum

Effective Date 1 September 2018

This Data Processing Addendum for the GDPR (**Addendum**) is made as of the Effective Date by and between Fresh Relevance Ltd incorporated and registered in England and Wales with company number 07754049 of 5 Benham Road, Southampton Science Park, Southampton, SO16 7QJ (**Provider**) and:

Name of Company:

Incorporated and registered in:

Country:

At the following address:
(**Customer**).

BACKGROUND

(A) The Customer and the Provider entered into an agreement for the provision of software as a service (**Master Agreement**) that may require the Provider to process Personal Data on behalf of the Customer.

(B) This Addendum sets out the additional terms, requirements and conditions that apply when the Provider processes Personal Data under the Master Agreement.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Addendum.

1.1 Definitions:

Business Purposes: the services described in the Master Agreement.

Data Subject: an individual who is the subject of Personal Data.

GDPR: means EU Regulation (2016/679).

Personal Data: means personal data (as the term "personal data" is defined under GDPR) processed by the Provider on behalf of the Customer in connection with the performance of the Master Agreement.

Processing, processes and process: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process.

Data Protection Legislation: all applicable privacy and data protection laws including the GDPR and any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (*2002/58/EC*) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*).

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Supervisory Authority: shall have the meaning as defined under GDPR.

1.2 This Addendum is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Addendum.

1.3 The Annexes form part of this Addendum and will have effect as if set out in full in the body of this Addendum. Any reference to this Addendum includes the Annexes.

1.4 A reference to writing or written includes faxes but not email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Addendum and any provision contained in the Annexes, the provision in the body of this Addendum will prevail; and

(b) any of the provisions of this Addendum and the provisions of the Master Agreement, the provisions of this Addendum will prevail.

2. Personal data types and processing purposes

2.1 This Addendum takes effect on the Effective Date.

2.2 The Customer and the Provider acknowledge that for the purpose of the Data Protection Legislation, the Customer is the controller and the Provider is the processor.

2.3 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

2.4 ANNEX A describes the subject matter, duration, nature and purpose of processing and the type of Personal Data and categories of Data Subject in respect of which the Provider may process to fulfil the Business Purposes of the Master Agreement.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes and in accordance with the Customer's written instructions.

3.2 The Provider may disclose Personal Data to third parties if required to do so by law. If a law, court, regulator or supervisory authority requires the Provider to process or disclose Personal Data, the Provider shall use reasonable endeavours to inform the Customer of the legal or regulatory requirement, unless the law prohibits such notice.

3.3 The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

4. Security

4.1 Taking into account:

(a) the nature, scope, context and purposes of processing;

(b) the state of the art and costs of implementation; and

(c) the risk of varying likelihood and severity for the rights and freedoms of individuals,

the Provider shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

4.2 The Provider shall implement measures, in accordance with clause 4.1, to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) Data minimization;

(b) the pseudonymisation and encryption of personal data;

(c) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(e) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

4.3 The Provider shall ensure:

(a) the reliability of any of the Provider’s employees who have access to the Personal Data;

(b) that access to the Personal Data is limited to:

(i) those employees who need access to the Personal Data to meet the Provider's obligations under this agreement; and

(ii) in the case of any access by any employee, such part or parts of the Personal Data as is strictly necessary for performance of that employee's duties,

(c) that all of its employees involved with the Services:

(i) are informed of the confidential nature of the Personal Data;

(ii) are informed of the laws relating to handling Personal Data; and

(iii) are aware both of the Provider's duties and their personal duties and obligations under such laws and this agreement.

5. Data subject requests

5.1 If Fresh Relevance receives a request from a Data Subject to invoke their GDPR rights, including access to, or deletion of that person's Personal Data, Fresh Relevance shall:

(a) notify the Customer within two Business Days of receiving the request;

(b) provide the Customer with full co-operation and assistance;

(c) communicate the name and contact details of the Provider's data protection officer or other contact point where more information can be obtained; and

(d) not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Customer.

6. Complaint, Notice, Communication or Personal Data Breach

6.1 If the Provider receives any complaint, notice or communication from a Data Subject or a Regulator which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the DPA and the data protection principles, or if the Provider becomes aware of any Personal Data Breach, it shall:

(a) notify the Customer quickly;

(b) provide the Customer with full co-operation and assistance; and

(c) communicate the name and contact details of the Provider's data protection officer or other contact point where more information can be obtained; and

(d) not disclose the Personal Data to any Data Subject or to a third party other than at the request of the Customer.

6.2 If the Provider becomes aware of a Personal Data Breach, it shall also, as soon as reasonably possible, provide the Customer with the following information:

(a) describe the nature of the Personal Data Breach, including, where possible the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) describe the likely consequences of the Personal Data Breach; and

(c) describe the measures taken, or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.3 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Provider will reasonably co-operate with the Customer in the Customer's handling of the matter, this may include where appropriate:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

7. Cross-border transfers of personal data

7.1 The Provider (or any sub-contractor) shall not transfer or otherwise process Personal Data outside the European Economic Area unless in accordance with the Customer’s instructions or consent.

8. Subcontractors

8.1 The Customer hereby authorizes the Provider to lease servers and related services from Amazon Web Services (AWS) in Ireland, under the standard published terms of AWS, and acknowledges that AWS is a third-party Data Processor.

8.2 In relation to other third-parties chosen by the Provider, it may only authorise a third party (subcontractor) to process the Personal Data:

(a) subject to the Customer's prior written consent;

(b) if provisions relating to data processing and data protection in the subcontractor's contract are on terms substantially the same as those between the Customer and the Provider, or

subject to the Customer's prior written consent that the subcontractor's contract is acceptable;

(c) providing the subcontractor's ability to process the Personal Data will end automatically, or be ended by the Provider, on termination of the Provider's agreement with the Customer.

8.3 If a subcontractor chosen by either party, the Customer or the Provider, fails to fulfil its obligations under the Data Processing Legislation, this is treated as if that party had failed to fulfil its obligations in the same way.

9. Data return and destruction

The Provider shall either, at the direction of the Customer, return or destroy all Personal Data on termination of this Addendum, except to the extent Data Protection Legislation requires the Provider to retain it. In that case, the Provider will no longer process Personal Data, except to the extent required by applicable Data Protection Legislation.

10. Audit

The Provider shall make available to the Customer all information necessary to demonstrate compliance with its obligations under Data Protection Legislation to allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

This Addendum has been entered into on the date stated at the beginning of it.

Signed by (Name):

for and on behalf of **Customer**

Director or other person authorised to bind customer.

Signed by Peter Austin

for and on behalf of **Fresh Relevance Ltd**

Director

ANNEX A Personal Data Processing Purposes and Details

Subject matter of processing: the performance of services pursuant to the Master Agreement

Duration of Processing: the duration of the Master Agreement

Nature of Processing: providing Services or fulfilling contractual obligations to the Customer (Controller) as described in the Master Agreement. Services may include the processing of Personal Data by the Provider (Processor) and/or its Approved Sub-processors on systems which may contain Personal Data.

Business Purposes: the provision of Services by the Provider to the Customer as specified in the Master Agreement

Type of Personal Data: data subjects' accounts, orders, interests, marketing seen or responded to, and other data useful for marketing and reports, but not special categories of personal data. The Customer can also instruct the Provider to store additional data and to import and export data to third-party systems.

Categories of Data Subject: the Customer's prospects, users, customers, employees, and other third parties.

Identify the legal basis for processing Personal Data outside the EEA in order to comply with cross-border transfer restrictions: the Provider processes data in the EEA, but if instructed by the Customer to transfer or process Personal Data outside the EEA, the Provider will use the legal basis supplied.

List of Approved Sub-processors: This list is incorporated by reference, so it can change as necessary. You can find it as follows: go to *https://www.freshrelevance.com/legal-documents*, look for Approved Sub-processors and click it.