Agility PR Solutions Data Processing Agreement Addendum

This Agility PR Solutions Data Processing Agreement Addendum governs the processing of Personal Data that Customer uploads or otherwise provides to Agility in connection with Agility's Products and Services, and the processing of any Personal Data that Agility uploads or otherwise provides to Customer in connection with its Products and Services. Terms not otherwise defined shall have the meaning set forth in the Agility Contract.

1. Definitions

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with Agility. "Control," for purposes of this definition, means the direct or indirect ownership or control of 50% or more of the stock or other equity interest entitled to vote for the election of directors or equivalent governing body.

"Agility Contract" means the Agility Terms and Conditions, Agility Order Form, Agility Enterprise Agreement and other agreement(s), as applicable, entered into between Agility and the Customer in which this DPA is incorporated by reference.

"Agility Group" means Agility and its Affiliates engaged in the Processing of Personal Data.

"Agreement" means this DPA together with the Agility Contract.

"Customer Personal Data" means Personal Data that Customer uploads or otherwise provides to Agility in connection with use of Agility's Products or Services, including, without limitation, information with regard to Customer's employees and users of Agility's Products and Services and any Personal Data of Journalists uploaded by Customer to the Agility Media Database.

"Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Processor"** means the entity which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data under this DPA, including, without limitation, the GDPR and UK DPA.

"**Data Subject"** means the identified or identifiable person to whom Personal Data relates.

"DPA" means this Data Processing Agreement Addendum.

"GDPR" means the General Data Protection 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.

"Journalist" means media professionals, journalists, editorial staff, media production staff, bloggers, twitterers, and social media commentators and other key influencers.

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

"Personal Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data stored or otherwise processed.

"Process" and "Processing" means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Subprocessor" means any Processor engaged by Agility or a member of the Agility Group.

"Supervisory Authority" means an independent public authority which is established by a European Union member state pursuant to Article 51 of the General Data Protection Regulation.

"UK DPA" means the United Kingdom's General Data Protection Regulation, tailored by the Data Protection Act 2018.

2. Processing of Personal Data

   2.1. Each of Agility and Customer acknowledge and agree that with regard to the Processing of Personal Data:

      (i) Customer is the Data Controller with respect to the Customer Personal Data, and Agility is the Data Processor with respect to the Customer Data.

      (ii) Agility is the Data Controller with respect to the Journalist Personal Data contained within the Agility Media Database and Customer is the Data Processor with respect to such Personal Data.

   2.2. Each party shall have sole responsibility for the accuracy and quality of the Personal Data it provides to the other party for Processing and the means by which the Personal Data was acquired, and shall comply with their respective obligations under the Data Protection Laws.

   2.3. Each party agrees to Process Personal Data received pursuant to the Agreement only for the purposes set forth in the Agreement (or as otherwise instructed in writing by the Data Controller), unless required by UK, EU or member state law to which the Data Processor is subject.

3. Details of the Processing

   3.1. Categories of Data Subjects: Customer's employees; Customer's users of Agility's Products and Services; Journalists

   3.2. Types of Personal Data:

      (i) Customer contact information, names, email addresses, phone numbers, user IDs, login information and other online identifiers.

      (ii) Journalist names, contact information, biographical information, career history, employment details, article headings and citations, social media handles, personal interests.

      (iii) It is not anticipated that special categories of Personal Data will be processed.

   3.3. Purpose, Nature and Subject Matter of the Processing: Personal Data will be Processed for the purposes of providing and receiving the Products and Services set forth in the Agility Contract.

4. Subprocessors

   4.1. With the exception of Subprocessors who form part of the Agility Group and Agility's current data center hosting provider and email distribution provider, to which Customer consents, neither party shall engage a Subprocessor to Process the Personal Data other than with the prior written consent of the Data Controller, such consent to be subject to the Data Processor meeting the conditions set out in all Data Protection Laws, including without limitation Article 28 (2) and (4) of the GDPR. Agility shall notify Customer of any intended additional Subprocessors, and will provide Customer the opportunity to reasonably object to the engagement of the new Subprocessor within 30 days of being notified. The objection must be based on reasonable grounds. If Agility and the Customer are unable to resolve the objection, either party may terminate the Agility Contract by providing written notice to the other party.

5. Security

   5.1. Each party shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and take all measures required pursuant to the Data Protection Laws, including without limitation Article 32 GDPR, in relation to the Processing of Personal Data, taking account of the

risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

5.2. Each party shall take all reasonable steps to ensure the reliability of persons authorised to Process the Personal Data and ensure that they have committed themselves to obligations of confidentiality.

6. Notifications to Data Controller

6.1. Each party in its capacity as Data Processor shall promptly notify the Data Controller, upon becoming aware of or reasonably suspecting a Personal Data Breach and shall, unless clause 6.2 below applies, provide the Data Controller at the time of original notification with sufficient information which allows the Data Controller to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum:

(i) describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

(ii) communicate the name and contact details of the Data Processor's Data Protection Officer or, where the Data Processor has not appointed a Data Protection Officer, the relevant contact from whom information may be obtained;

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

(iv) describe the measures taken or proposed to be taken to address the Personal Data Breach.

6.2 If at the time of making the original notification described in Section 6.1 the Data Processor does not have available to it all the information described in Sections 6.1(i) - (iv), the Data Processor shall include in the original notification such information as it has available to it at that time, and then shall provide the further information set out in Sections 6.1(i) - (iv) as soon as possible thereafter.

7. Assistance to the Data Controller

7.1. Each party in its capacity as Data Processor shall:

(i) assist the Data Controller in ensuring compliance with the obligations pursuant to all Data Protection Laws, including without limitation Articles 35 and 36 of the GDPR, taking into account the nature of Processing and the information available to the Data Processor;

(ii) at the choice of the Data Controller, delete or return all the personal data to the Data Controller after the end of the provision of Services relating to the Processing;

(iii) make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in all Data Protection Laws, including without limitation Article 28 of the GDPR, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller to the extent reasonably required for verifying compliance with (i) Data Protection Laws in relation to the Processing of Personal Data under this Agreement; and (ii) the requirements of this Agreement. Any audit or inspection shall be subject to an agreement to maintain the confidentiality of all proprietary and confidential information of the party to be audited, and shall be reasonable in scope and duration in relation to the purpose for which the audit or inspection is conducted.

8. Data Transfers

8.1. For transfers of EU Personal Data or UK Personal Data to a party for Processing in their capacity as Data Processor in a jurisdiction other than a jurisdiction in the EU, the EEA, the UK, or the European Commission-approved countries providing 'adequate' data protection, each party agrees that (a) with respect to EU Personal Data it will enter into the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent version which replaces these (the "Standard Clauses"); and (b) with respect to UK

Personal Data it will enter into the Standard Contractual Clauses (Processors) as laid down in the Commission Decision 2010/87 EU of 5 February 2010, or any subsequent revised clauses or safeguards as required or permitted by the UK DPA (the "UK Clauses").

8.2. Without prejudice to the generality of Section 8.1, with effect from the commencement of any transfer of EU Personal Data or UK Personal Data, the parties agree that the Standard Clauses and/or UK Clauses shall apply, as applicable, (and shall be deemed to have been entered into by the Data Controller (as "data exporter") and the Data Processor (as "data importer") in respect of any transfer of Personal Data outside the European Economic Area or the United Kingdom from the relevant Data Controller to the Data Processor (or onward transfer) where such transfer outside the European Economic Area or the United Kingdom would otherwise be prohibited by the Data Protection Laws. In such event the Standard Clauses and/or UK Clauses, as applicable, as set forth in the Annexes to this DPA, shall be deemed to form an integral part of this DPA.

8.3. If data transfers under this Section 8 of the DPA rely on Standard Clauses and/or UK Clauses to enable the lawful transfer of EU Personal Data or UK Personal Data, as set forth in the preceding Section, the parties agree that Data Subjects for whom a party in their capacity as Data Processor processes EU Personal Data or UK Personal Data are third-party beneficiaries under the Standard Clauses and/or UK Clauses, as applicable.

9. Term

9.1. This DPA shall remain in full force and effect until termination of the Agility Contract, and until all Personal Data has been returned or deleted in accordance with Section 7.1 above.

10. Governing Law, Jurisdiction and Venue

10.1. Notwithstanding anything in this DPA to the contrary, this DPA will be governed by and construed in accordance with English law regardless of the laws that might otherwise govern under applicable choice-of-law principles. If any provision of this DPA is held invalid, illegal, or unenforceable, the remaining provisions will continue unimpaired. The parties consent to the jurisdiction of the courts of England with respect to any legal proceedings in connection with this DPA.

11. Order of Precedence

11.1. In the event of any conflict or inconsistency between any of the terms of the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) this DPA; and (b) the Agility Contract. Terms not otherwise defined shall have the meaning set forth in the Agility Contract.

Annex A

Standard Clauses and UK Clauses

The parties agree that when the transfer of Personal Data from Agility (the controller) to the Customer (the processor) occurs pursuant to Section 8 of the DPA with respect to EU Personal Data, the transfer shall be subject to the Standard Clauses completed as follows:

1. Module Two will apply;
2. In Clause 7, the optional docking clause will apply;
3. In Clause 9 Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set forth in Section 4.1 of this DPA;
4. In Clause 11, the optional language will not apply;
5. In Clause 17, Option 1 will apply, and the Standard Clauses shall be governed by Irish law; and
6. In Clause 18(b), disputes shall be resolved before the courts of Ireland;
7. Annex I of the Standard Clauses shall be deemed completed with the information set out in Annex I to this DPA; and
8. Annex II of the Standard Clauses shall be deemed completed with the information set out in Annex II to this DPA

The parties agree that when the transfer of Personal Data from Agility (the controller) to the Customer (the processor) occurs pursuant to Section 8 of the DPA with respect to UK Personal Data, the transfer shall be subject to the UK Clauses completed as follows:

1. Appendix 1 shall be deemed completed with the relevant information set out in Annex I to this DPA;
2. Appendix 2 shall be deemed completed with the relevant information set out in Annex II to this DPA; and
3. The optional illustrative indemnification clause will not apply.
4. The UK Clauses shall be governed by English law and disputes shall be resolved before the Courts of England and Wales.

In the event of any conflict between the DPA and the and Standard Clauses or UK Clauses, the Standard Clause or UK Clauses, as applicable, shall prevail to the extent of such conflict.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Agility PR Solutions Limited

Address: Tayfield House, Poole Road, Bournemouth, Dorset, England, United Kingdom, BH4 9DW

Contact person's name, position and contact details: Allison Murphy, Managaing Director, allison.murphy@agilitypr.com.

Activities relevant to the data transferred under these Clauses: Agility is a provider of a global media database containing journalist contact information.

Signature and date:

Role (controller/processor): controller

Data importer(s):

Name: The Customer identified in the Agility Contract.

Address: The Customer's address specified in the Agility Contract.

Contact person's name, position and contact details: The Customer's contact information specified in the Agility Contract.

Activities relevant to the data transferred under these Clauses: The data importer is a customer of Agility's global media database.

Signature and date:

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Journalists, which include media professionals, editorial staff, media production staff, bloggers, twitterers, and social media commentators and other key influencers.

Categories of personal data transferred

Journalist names, contact information, biographical information, career history, employment details, article headings and citations, social media handles, personal interests.

Sensitive data transferred (if applicable) and applied restrictions or safeguards

Not applicable.

The frequency of the transfer

At data importer's discretion in using the Agility Products and Services during the term of the Agility Contract.

Nature of the processing

Sending of news releases by the data importer to journalists to develop and cultivate relationships within targeted industries relevant to the data importer, solely in accordance with the terms of Agility Contract.

Purpose(s) of the data transfer and further processing

To enable the data importer to utilize the data exporter's Products and Services.

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

Subject to Section 9 of the DPA, the personal data will be retained as needed to utlize the data exporter's Products and Services during the term of the Agility Contract.

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

C. COMPETENT SUPERVISORY AUTHORITY

Where the UK Clauses are applicable the Information Commissioner's Office shall act as the competent supervisory authority.

Where the Standard Clauses are applicable:

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer 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 application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 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 application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located shall act as competent supervisory authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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, the following describes the data importer's technical and organizational security measures:

Measures for user identification and authorization	Only licensed users within the Data Importer's organization are permitted to access the data and process the data within the Agility Product. Each licensed user is required to have a user name and password to access the Agility Product. Level of user access is designated at Admin or non-Admin.
Measures of encryption of personal data	Data is encrypted in flight using industry standard encryption technologies (SSL, TLS 1.2). Passwords are encrypted at rest.
Measures for protection of data	Data importer maintains a commercially reasonable level of physical and electronic security as to the Equipment, Permitted User accounts, passwords, Product, Software and Services in its control and which it uses process the data, and for ensuring no unauthorized use of the same. Data Importer may not provide any data in any form to a party who is not a licensed user of the Agility Product.
Measures for ensuring data minimization and limited data retention	The amount of data that Data Importer can export from the Agility Product is limited pursuant to the Agility Contract. Data importer must fully delete all data exported from the Agility Product within 30 days from the date of download.
Measures for ensuring data accuracy	Data Importer is required to export an updated download immediately prior to sending any news release to a journalist. Data Importer is required to manage and maintain a register of journalists who have previously unsubscribed from receiving news releases from Data Importer, and is prohibited from sending any emails to an unsubscribed journalist.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Agility utilizes network security controls including firewall and UTM devices and other traffic and event correlation procedures designed to protect its systems from intrusion and limit the scope of any successful attack. Regular vulnerability assessments, patch management and threat protection technologies and scheduled monitoring procedures are designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code/bad actors.

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	Agility maintains business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors: _____