DATA PROTECTION ADDENDUM

From May 20, 2018

InLinkz - Aris Kormpetis (“**Company**”) and the legal entity that entered into an agreement for the provision of the services (the “**Services**” and the “**Agreement**”, respectfully) regardless of the form of organization (“**Customer**”), are agreeing to these Data Protection Terms (“**DPA**”). This DPA is entered into by Company and Customer and supplement the Agreement. This DPA will be effective, and replace any previously applicable terms relating to their subject matter, from the Terms Effective Date.

The customer agreeing to these when start using the Services. If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

1. Introduction

1.1. This DPA reflects the parties’ agreement on the processing of Personal Data in connection with the Data Protection Laws.

1.2. Any ambiguity in this DPA shall be resolved to permit the parties to comply with all Data Protection Laws.

1.3. In the event and to the extent that the Data Protection Laws impose stricter obligations on the parties than under this DPA, the Data Protection Laws shall prevail.

2. Definitions and Interpretation

2.1. In this DPA:

2.1.1. “**Affiliate**” means an entity that directly or indirectly controls, is controlled by, or is under common control with, a party.

2.1.2. “**Data Protection Laws**” means, as applicable, any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the 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 (“GDPR”).

2.1.3. “**Data Subject**” means a data subject to whom Personal Data relates.

2.1.4. “**Personal Data**” means any personal data that is processed by a party under the Agreement in connection with its provision or use (as applicable) of the Services.

2.1.5. "**Security Incident**" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Personal Data Breach will comprise a Security Incident

2.1.6. “**Terms Effective Date**” means 25 May 2018.

2.1.7. The terms "**controller**", "**processing**" and "**processor**" as used in this have the meanings given in the GDPR.

2.1.8. Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3. Application of this DPA

3.1. This DPA will only apply to the extent all of the following conditions are met:

3.1.1. Company processes Personal Data that is made available by the Customer in connection with the Agreement;

3.1.2. The Data Protection Laws applies to the processing of Personal Data.

3.2. This DPA will only apply to the Services for which the parties agreed earlier including Terms of Use and Privacy Policy which incorporates the DPA by reference.

4. Roles and Restrictions on Processing

4.1. **Independent Controllers**. Each party:

4.1.1. is an independent controller and processor of Personal Data under the Data Protection Laws;

4.1.2. will individually determine the purposes and means of its processing of Personal Data; and

4.1.3. will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of Personal Data.

4.2. **Restrictions on Processing**. Section 4.1 (Independent Controllers) will not affect any restrictions on either party's rights to use or otherwise process Personal Data under the Agreement.

4.3. **Sharing of Personal Data**. In performing its obligations under the Agreement, a party may provide Personal Data to the other party. Each party shall process Personal Data only for (i) the purposes set forth in the Agreement or as (ii) otherwise agreed to in writing by the parties, provided such processing strictly complies with (iii) Data Protection Laws, (ii) Relevant Privacy Requirements and (iii) its obligations under this Agreement (the "**Permitted Purposes**").

4.4. **Lawful grounds and transparency**. Each Party shall maintain a publicly-accessible privacy policy on its websites that is available via a prominent link that satisfies transparency disclosure requirements of Data Protection Laws. Each Party warrants and represents that it has provided Data Subjects with appropriate transparency regarding data collection and use and all required notices and obtained any and all consents or permissions necessary under e-Privacy Law. It is hereby clarified that Customer is the initial Controller of Personal Data. Where Customer relies on consent as its legal basis to Process Personal Data, it shall ensure that it obtains a proper affirmative act of consent from Data Subjects in accordance with Data Protection Law in order for itself and the other Party to Process such Personal Data as set out herein. The foregoing shall not derogate from Company's responsibilities under the Data Protection Laws (such as the requirement to provide information to the data subject when the Personal Data in connection with the processing of Personal Data.

4.5. **Data Subject Rights**. It is agreed that where either party receives a request from a Data Subject in respect of Personal Data controlled by such Party, then such Party shall be responsible to exercise the request, in accordance with Data Protection Laws.

5. Personal Data Transfers

5.1. **Transfers of Personal Data Out of the European Economic Area**. Either party may transfer Personal Data outside the European Economic Area if it complies with the provisions on the transfer of personal data to third countries in the Data Protection Laws (such as through the use model clauses or transfer of Personal Data to jurisdictions as may be approved as having

adequate legal protections for data by the European Commission).

6. Protection of Personal Data.

6.1. The parties will provide a level of protection for Personal Data that is at least equivalent to that required under Data Protection Laws. Both parties shall implement appropriate technical and organisational measures to protect the Personal Data. In the event that a party suffers a confirmed Security Incident, each party shall notify the other party without undue delay and the parties shall cooperate in good faith to agree and action such measures as may be necessary to mitigate or remedy the effects of the Security Incident.

7. Priority

7.1. **Effect of this DPA**. If there is any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement then, the terms of this DPA will govern. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

8. Changes to this DPA.

8.1. Company may change this DPA if the change is required to comply with Data Protection Laws, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the parties as independent controllers of Personal Data under the Data Protection Laws; (ii) expand the scope of, or remove any restrictions on, either party's rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.

8.2. **Notification of Changes**. If Company intends to change this DPA under this Section, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

For Company:	For Customer:
By: InLinkz - Aris Kormpetis	By: _____
Name: Aris Korbetis	Name: _____
Title: Director	Title: _____
Date: May 23rd, 2018	Date: _____
Signature:	Signature: _____