This Data Protection Addendum ("**Addendum**") forms part of Company's Terms of Use available at https://fiksu.com/terms-of-use/ as may be amended or replaced from time to time and is incorporated into all current and future agreements between the parties ("**Principal Agreement**") between: (i) **GDMservices, Inc. d/b/a FiksuDSP** (the "**Company**") acting on its own behalf and as agent for each Company's Affiliates acting on its own behalf and as agent for each Company's Affiliates; and (ii) you (the "**Client**") accepting the Principal Agreement acting on your own behalf and as agent for each of your Affiliates.

IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND YOUR AFFILIATES TO THE PRINCIPAL AGREEMENT AND ANY TERMS HEREOF. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE TO THE PRINCIPAL AGREEMENT AND ANY TERMS HEREOF, YOU MUST NOT ACCEPT THIS PRINCIPAL AGREEMENT AND MAY NOT USE THE SERVICE.

For the purposes of this Agreement the Client is a Controller and the Company is a Processor.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Controller Personal Data in respect of which any Controller Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which any Controller Group Member is subject to any other Data Protection Laws;

1.1.2 "**Controller Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Controller, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Controller Group Member**" means Controller itself or any Controller Affiliate;

1.1.4 "**Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Controller Group Member pursuant to or in connection with the Principal Agreement;

1.1.5 "**Contracted Processor**" means Processor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Controller Personal Data from any Controller Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Controller Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below; *For the avoidance of doubt:* (a) without limitation to the generality of the foregoing, the parties to this Addendum intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12; and (b) where a transfer of Personal Data is of a type authorised by Data Protection Laws in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer;

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controller Group Members pursuant to the Principal Agreement;

1.1.12 **"Standard Contractual Clauses"** means the contractual clauses set out in COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593)(Text with EEA relevance)(2010/87/EU) and under section 13.4;

1.1.13 "**Subprocessor**" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to Process Personal Data on behalf of any Controller Group Member in connection with the Principal Agreement; and

1.1.14 "**Processor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Processor warrants and represents that, before any Processor Affiliate Processes any Controller Personal Data on behalf of any Controller Group Member, Processor's entry into this Addendum as agent for and on behalf of that Processor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Processor Affiliate.

3. Processing of Controller Personal Data

3.1 Processor and each Processor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Controller Personal Data; and

3.1.2 not Process Controller Personal Data other than on the relevant Controller Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Processor or the relevant Processor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Controller Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Controller Group Member:

3.2.1 instructs Processor and each Processor Affiliate (and authorises Processor and each Processor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Controller Personal Data; and

3.2.1.2 in particular, transfer Controller Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Controller Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Controller Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Controller may make reasonable amendments to Annex 1 by written notice to Processor from time to time as Controller reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Processor and Processor Affiliate Personnel

Processor and each Processor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Controller Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Controller Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor and each Processor Affiliate shall in relation to the Controller Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Processor and each Processor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Subprocessing**

6.1 Each Controller Group Member authorises Processor and each Processor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6 and any restrictions in the Principal Agreement.

6.2 Processor and each Processor Affiliate may continue to use those Subprocessors already engaged by Processor or any Processor Affiliate as at the date of this Addendum, subject to Processor and each Processor Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 Processor shall give Controller prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within thirty (30) calendar days of receipt of that notice, Controller notifies Processor in writing of any objections (on reasonable grounds) to the proposed appointment:
Neither Processor nor any Processor Affiliate shall appoint (nor disclose any Controller Personal Data to) the proposed Subprocessor except with the prior written consent of Controller.

6.4 With respect to each Subprocessor, Processor or the relevant Processor Affiliate shall:

6.4.1 before the Subprocessor first Processes Controller Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Controller Personal Data required by the Principal Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) Processor, or (b) the relevant Processor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Controller Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

6.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Processor, or (b) the relevant Processor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Controller Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Controller Group Member(s) (and Controller shall procure that each Controller Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution); and

6.4.4 provide to Controller for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Controller may request from time to time.

6.5 Processor and each Processor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Controller Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Processor.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Processor and each Processor Affiliate shall assist each Controller Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller Group Members' obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Processor shall:

7.2.1 promptly notify Controller if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Controller Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Controller or the relevant Controller Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

8. **Personal Data Breach**

8.1 Processor shall notify Controller without undue delay upon Processor or any Subprocessor becoming aware of a Personal Data Breach affecting Controller Personal Data, providing Controller with sufficient information to allow each Controller Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

Such notification shall as a minimum:

8.1.1 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;

8.1.2 communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;

8.2 Processor shall co-operate with Controller and each Controller Group Member and take such reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Processor and each Processor Affiliate shall provide reasonable assistance to each Controller Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required of any Controller Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Controller Personal Data

10.1 Subject to sections 10.2 and 10.3 Processor and each Processor Affiliate shall promptly and in any event within five (5) business days of the date of cessation of any Services involving the Processing of Controller Personal Data (the "**Cessation Date**"), delete (for avoidance of any doubt, "*delete*" here means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed) and procure the deletion of all copies of those Controller Personal Data.

10.2 Subject to section 10.3, Controller may in its absolute discretion by written notice to Processor within five (5) business days of the Cessation Date require Processor and each Processor Affiliate to (a) return a complete copy of all Controller Personal Data to Controller by secure file transfer in such format as is reasonably notified by Controller to Processor; and (b) delete and procure the deletion of all other copies of Controller Personal Data Processed by any Contracted Processor. Processor and each Processor Affiliate shall comply with any such written request within five (5) business days of the Cessation Date.

10.3 Each Contracted Processor may retain Controller Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Processor and each Processor Affiliate shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Processor shall provide written certification to Controller that it and each Processor Affiliate has fully complied with this section 10 within ten (10) business days of the Cessation Date.

11. Audit rights

11.1 Subject to sections 11.2 to 11.3, Processor and each Processor Affiliate shall make available to each Controller Group Member on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Controller Group Member or an auditor mandated by any Controller Group Member in relation to the Processing of the Controller Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Controller Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Controller or the relevant Controller Affiliate undertaking an audit shall give Processor or the relevant Processor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it

cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Controller or the relevant Controller Affiliate undertaking an audit has given notice to Processor or the relevant Processor Affiliate that this is the case before attendance outside those hours begins; or

11.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

11.3.3.1 Controller or the relevant Controller Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Processor's or the relevant Processor Affiliate's compliance with this Addendum; or

11.3.3.2 A Controller Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory, where Controller or the relevant Controller Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Processor or the relevant Processor Affiliate of the audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.3, each Controller Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Controller Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 Processor warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a Processor Affiliate, Processor's or the relevant Processor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf of that Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Subprocessor.

12.5 It is hereby agreed that data exporter and data importer will mutually exchange with such information necessary for the Standard Contractual Clauses as:

- Name of the data exporting organization, address, telephone number, fax (if applicable), email – for data exporter; and
- Name of the data importing organization, address, telephone number, fax (if applicable), email – for data importer.

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum,

including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

13.2 Nothing in this Addendum reduces Processor's or any Processor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Processor or any Processor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Controller may:

13.4.1 by at least 30 (thirty) calendar days' written notice to Processor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Controller reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Controller gives notice under section 13.4.1:

13.5.1 Processor and each Processor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and

13.5.2 Controller shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Processor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 and/or 13.5.1.

13.6 If Controller gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Controller's notice as soon as is reasonably practicable.

13.7 Neither Controller nor Processor shall require the consent or approval of any Controller Affiliate or Processor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

i. Subject matter and duration of the Processing of Controller Personal Data:

The subject matter of this Addendum is the processing of Personal Data in connection with the Services provided to the Controller. As between parties, the duration of the data processing under this Addendum is until the termination of the Principal Agreement in accordance with its terms, except as otherwise required by applicable law or as instructed by the Controller plus for about 24 months during which Processor stores the pseudonymized data, let alone special requirement provided by GDPR (fraud, legal claim, etc.). Other than that, all personal data is deleted once the 24-month period is over.

ii. The nature and purpose of the Processing of Controller Personal Data:

The purpose of the data processing under this Addendum is the provision of the Services and the performance of each party's obligations under the Principal Agreement (including this Addendum) or as otherwise agreed by the parties in mutually executed written form. Processor provides marketing technology solutions and other Services as described in the Principal Agreement and may process Personal Data in connection with the Services provided to, and upon the instruction of the Controller.

Processor buys mobile advertising space on behalf of Processor' clients which are generally mobile application providers and companies looking to advertise via mobile applications. When Data Subject clicks on a client ad or application link delivered by Processor, its servers receive and store a mobile identifier ("Mobile ID") which is a pseudonymous number that is associated with your mobile device.

In addition to the Mobile ID, Processor collect information about the kind of mobile device which Data Subject use, the operating system for the mobile device of Data Subject, IP address, the applications which Data Subject download from clients of the Processor when, how, and how often Data Subject uses those applications.

Processor uses device's Mobile ID of Data Subject and other information about client applications which Data Subject download to help the clients of Processor understand which ads are most effective at generating downloads of applications of Processor' clients. Processor also use Mobile ID of Data Subject and the information associated with device Mobile ID of Data Subject over time to enhance services of Processor and to select ads of Processor' clients that are most likely to be of interest to Data Subject.

Processor may aggregate data of Data Subject with other customers' data in non-personally identifiable, aggregated, and de-identified form to better optimize marketing campaigns and to improve the website or service of Processor. Processor may also share this de-identified aggregate data publicly, for example in order to provide analytical summaries.

iii. The types of Controller Personal Data to be Processed:

Mobile advertising data includes: Mobile ID, IP address, User Agent, other data from OpenRTB, Ad Exchange RTB and other RTB exchange specific protocols.

Event tracking data includes: Mobile ID, IP address, User Agent.

Mobile ID is one of:
- Apple IDFA - https://developer.apple.com/documentation/adsupport/asidentifiermanager/1614151-advertisingidentifier
- Google Advertising ID - GAID - https://support.google.com/googleplay/android-developer/answer/6048248?hl=en
- Android ID (for very old integrations)
- Device ID (for very old integrations)

iv. The categories of Data Subject to whom the Controller Personal Data relates:

Internet users - anyone who's accessing or using the Website* and/or interacting with Application Marketing Service**;
Clients - authorized users of Application Marketing Service.

***Website:**
Client registration data includes: name, e-mail, address, IP address
Domains/pages:

https://fiksu.com/get-started
https://fiksu.com/contact-us
https://dashboard.fiksu.com/en/signin
https://support.fiksu.com
https://support-cdn.fiksu.com
https://jira.fiksu.com (password protected)
https://confluence.fiksu.com (password protected)

****Application Marketing Service:**

Processor buys mobile advertising space on behalf of Processor' clients which are generally mobile application providers and companies looking to advertise via mobile applications. Mobile advertising data includes: Mobile ID, IP address, User Agent, other data from OpenRTB, Ad Exchange RTB and other RTB exchange specific protocols.

RTB end-point domains: adx.fiksu.com, adxs.fiksu.com, aerserv.fiksu.com, applovin.fiksu.com, mopub.fiksu.com, mopub23.fiksu.com, nexage23.fiksu.com, omax.fiksu.com, smaato.fiksu.com

Event tracking data includes: Mobile ID, IP address, User Agent.
Pre-install event tracking domains: ri.fiksu.com, ris.fiksu.com, b.fiksu.com, bs.fiksu.com, rc.fiksu.com, rcs.fiksu.com, handler.fiksu.com, pt.fiksu.com, asotrack1.fiksu.com, asotrack2.fiksu.com
Post-install and conversion event tracking domains: a.fiksu.com, sdk.fiksu.com, pt.fiksu.com
Other event tracking domains (with no personal data processing): er.fiksu.com, ers.fiksu.com, rn.fiksu.com, rns.fiksu.com
Opt-out data includes: Mobile ID
Opt-out page: https://fiksu.com/end-user-opt-out/
Other ad serving domains (with no personal data processing): ads.fiksu.com, rtb-creatives.fiksu.com, media.fiksu.com

v. **The obligations and rights of Controller and Controller Affiliates:**

Are set out in the Principal Agreement and this Addendum.