Data Processing Agreement

THIS DATA PROCESSING AGREEMENT (HEREINAFTER REFERRED TO AS THE "DPA") including its attachments and annexes forms part of, and is subject to, the ADIKTEEV General Terms and Conditions and other terms and conditions that reference the General Terms and Conditions or are incorporated into the General Terms and Conditions by reference, an Insertion Order, or other written or electronic terms of service or subscription agreement for the provision of the Services by ADIKTEEV that incorporates this DPA by reference (the "Principal Agreement") between the ADIKTEEV entity that is a Party to such Agreement ("ADIKTEEV") and the legal entity defined as 'Client' thereunder, together with all Client Affiliates (when and if applicable), (collectively, for purposes of this DPA, "Client"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

For purposes of the Agreement, Client shall act as a "Business" and/or "Controller" and ADIKTEEV shall act as a "Service Provider" and/or "Processor" of Client Personal Data under Data Protection Laws. Each party shall comply with Data Protection Laws.

The Client Data Controller has selected the Data Processor to act as a Service Provider in accordance with Art. 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, with repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR"),with the California Consumer Privacy Act of 2018, as amended, and with the Personal Information Protection Act ("PIPA") of 2011 as amended . In this context, the Parties agree to sign this DPA in order to define the data protection obligations of the Parties.

This DPA supersedes all provisions regarding the protection of personal data in the Principal Agreement and all previous contracts signed between the Parties regarding the protection of personal data.

If you are an individual who consents to the terms of this DPA on behalf of a business, you represent and warrant that you have the authority to bind that business to this DPA and your consent to this DPA will be treated as the consent of the business.

Electronic signatures express the consent for this DPA to be legally binding to the Parties and to serve as evidence on the same account as a hand-signed paper document.

1. DEFINITIONS

Capitalized terms used herein and not defined herein will have the meaning set forth in the Principal Agreement.

1.1. The terms "**Personal Data**", "**Processing**", "**Recipient**", "**Consent**", "**Supervisory Authority**" and "**Personal Data Breach**" have the same meaning as in the GDPR and all related terms should be interpreted accordingly.

1.2. The Terms "**Service Provider**", "**Personal Information**", "**Business Purpose**", "**Verifiable Consumer Request"** have the same meaning as in the CCPA and all related terms should be interpreted accordingly.

1.3. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

1.4. "**Applicable Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States, the Republic of Korea applicable to the Processing of

Personal Data under the Principal Agreement.

1.5. "**CCPA**" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations or guidance provided by the California Attorney General.

1.6. "**Contracted Business Purpose**" means the Service(s) as described in the section 4 and Annex 1 of this DPA for which the Data Processor receives or accesses the Personal Data.

1.7. "**Data Controller Personal Data**" means any Personal Data made available or transferred by the Data Controller or on behalf of the Data Controller by a third party to ADIKTEEV and any Personal Data that ADIKTEEV processes as "data processor".

1.8. "**Data Subject**" means (i) an identified or identifiable natural person who is in the European Economic Area or whose rights are protected by the GDPR; or (ii) a "Consumer" as the term is defined in the CCPA, or "Subject of Personal Information" as defined in article 2 of PIPA.

1.9. "**Data Subject Rights"** means those rights identified in the GDPR, the CCPA and the PIPA granted to Data Subjects.

1.10. "**GDPR**" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.11. "**PIPA**" means the Personal Information Protection Act effective in the Republic of Korea as of 2011, and as amended from time to time.

1.12. "**Standard Contractual Clauses**" means the agreement that could be executed by and between the Parties or between the Data Processor and a sub-processor pursuant to the European Commission's decision (EU) 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.

1.13. "**Sub-processors**" means any person appointed (including any third party but excluding independent contractors of Data Processor subject to Section 8 of this DPA) by or on behalf of the Data Processor or any Data Processor Affiliate to process Client Personal Data in accordance with the Principal Agreement.

2. SUBJECT MATTER OF THE DPA

2.1. This DPA sets forth the general terms and conditions under which the Data Processor shall process the Data Controller Data transferred by the Data Controller, its subsidiaries, its partners or any third party acting on behalf of the Data Controller to the Data Processor in the scope of the Principal Agreement for the performance of the Contracted Business Purposes.

2.2. Data Processor shall not process Data Controller Personal Data other than on what is agreed within this contract or the Data Controller's further instructions.

3. DURATION

3.1. This DPA shall come into effect from the effective date of the Principal Agreement.

3.2. The duration of this DPA is the duration of the provision of the Contracted Business Purpose(s).

3.3. Upon termination of this DPA, upon the Data Controller's written request, or upon fulfillment of all purposes agreed in the context of the Contracted Business Purpose(s) whereby no further processing is required, the Processor shall delete all Personal Data.

4. PROCESSING OF PERSONAL DATA

4.1. Processing of Personal Data

When Processing solely on Data Controller's behalf under the Principal Agreement, Data Processor shall Process Personal Data for the following purposes: (i) Processing in accordance with the Principal Agreement and this DPA; (ii) Processing for the Contracted Business Purpose(s); (iii) Processing to comply with Data Controller's reasonable and documented instructions, where such requests are consistent with the terms of the Principal Agreement, regarding the manner in which the Processing shall be performed; (iv) rendering Personal Data pseudonymized or fully anonymous, non-identifiable and non-personal; (v) Processing as required under any applicable laws to which Data Processor is subject; in such a case, Data Processor shall inform Data Controller of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

To the extent that Data Processor cannot comply with an instruction from Data Controller, Data Processor (i) shall inform Data Controller, providing relevant details of the problem, (ii) Data Processor may, without any kind of liability to Data Controller, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend access to the Client's account, and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Data Controller may, as its sole remedy, terminate the Principal Agreement and this DPA with respect to the affected Processing, and Data Controller shall pay to Data Processor all the amounts owed to Data Processor or due before the date of termination. Data Controller will have no further claims against Data Processor (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

4.2. Details of the Processing

The subject-matter of Processing of Personal Data by Processor is the performance of the Contracted Business Purposes pursuant to the Principal Agreement. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 (Details of the Processing) to this DPA.

Depending on the Principal Agreement, the main purpose of the Processing may be to deliver relevant ads to mobile app end-users and/or provide predictive analytics to improve marketing campaign performance.

5. DATA CONTROLLER'S OBLIGATIONS

The Data Controller notably warrants that prior to any transfer of Personal Data to the Data Processor, it has informed the Data Subject(s) according to Art. 13 GDPR, and/or has obtained prior explicit consent from the Data Subject as per Art 15 and Art 17 of PIPA, and/or has complied with any notification and/or registration obligations set forth by the Applicable Data Protection Laws.

The Data Controller guarantees that the intended purposes of the transfer and processing have been communicated to the Data Subject(s) upon the collection of the Personal Data.

The Data Controller warrants that it has all necessary rights to provide the Personal Data to the Data Processor for the Processing to be performed in relation to the Contracted Business Purpose(s) whether the data is collected directly by the Data Processor via a proprietary SDK or transferred by the Data Controller or a third party in the name and on behalf of the Data Controller. To the extent required by Applicable Data Protection

Law, the Data Controller is responsible for ensuring that any necessary Data Subject Consents to this Processing are obtained, and for ensuring that a record of such consents is maintained and will be shared with the Data Processor upon first request. Should such a consent be revoked by the Data Subject, the Data Controller is responsible for communicating the fact of such revocation to the Data Processor, and the Data Processor remains responsible for implementing any Controller instruction with respect to the further processing of that Personal Data.

The Data Controller is entitled to issue instructions concerning the Personal Data Processing in writing.

The Data Controller is responsible for responding to Data Subject requests notably related to Data Subjects Rights using its own access to the relevant Personal Data.

The Data Controller shall inform the Data Processor without undue delay if it is not able to comply with its responsibilities under this Section 5 or Applicable Data Protection Laws.

The Data Controller must notify the Data Processor if a Data Subject has exercised their CCPA right to opt-out of the sale of their Personal Data.

The Data Controller must notify the Data Processor immediately of any errors or irregularities that it is aware of regarding the processing of Personal Data by the Data Processor.

6. DATA PROCESSOR'S OBLIGATIONS

6.1. General obligations

The Data Processor undertakes in particular to comply with the conditions and/or the purpose of the Processing concerning the Personal Data which was communicated by the Data Controller or to which access will be given.

The Data Processor will only collect, use, retain, or disclose Personal Data necessary to perform the Contracted Business Purposes for which Data Controller provides or permits Personal Data access.

The Data Processor will not collect, use, retain, disclose, sell, or otherwise make Personal Data available for Data Processor's own commercial purposes or in a way that does not comply with the Applicable Data Protection Laws. If a law requires the Data Processor to disclose Personal Information for a purpose unrelated to the Contracted Business Purpose, the Data Processor must first inform the Client of the legal requirement and give Client an opportunity to object or challenge the requirement, unless the law prohibits such notice.

The Data Processor will limit Personal Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible operational purpose.

The Data Processor must promptly comply with any Client's request or instruction requiring the Data Processor to provide, amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized processing.

Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved Sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

6.2. CCPA obligations

If, pursuant to the CCPA and Section 6 of this DPA, the Data Controller notifies the Data Processor that a Data Subject has exercised its CCPA rights to opt-out of the sale of their personal information with the business, the Data Processor shall comply with the same obligation to not sale the Data Subject's Personal Information.

The Data Processor certifies that it understands this DPA and the CCPA's restrictions and prohibitions on selling personal information and retaining, using, or disclosing personal information outside of the Parties' direct business relationship, and it will comply with them.

The Data Processor warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing under this DPA.

The Data Processor must promptly notify the Client of any changes to the CCPA's requirements that may adversely affect its performance under the DPA.

6.3 PIPA obligations

Upon discovering a divulgence of personal information, the Data Processor will immediately inform the Data Controller, which commits to take the following actions:

- inform affected data subjects within 72 hours
- Report to the Personal Information Privacy Commission (PIPC), or the Korea Internet & Security Agency (KISA) within 72 hours if the divulgence involves:
    - ➔ Personal information of 1,000 or more individuals.
    - ➔ Sensitive or personally identifiable information.
    - ➔ Unlawful external access

7. COOPERATION BETWEEN THE PARTIES

Both parties will comply with all applicable requirements of the Applicable Data Protection Laws, including when applicable GDPR, the CCPA, and the PIPA when collecting, using, retaining, or disclosing personal information.

The Data Processor will reasonably cooperate and assist the Data Controller with meeting the Client's compliance obligations and responding to data protection-related inquiries, including responding to Data Subjects Rights or CCPA Verifiable Consumer Requests, taking into account the nature of the Data Processor's processing and the information available to the Data Processor.

The Data Processor must notify the Data Controller immediately if it receives any complaint, notice, or communication that directly or indirectly relates to either party's compliance with the Applicable Data Protection Laws.

The Data Processor shall notably assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights under the GDPR, the CCPA and the PIPA

If, pursuant to the CCPA, the Data Processor receives a Request to know or a Request to delete from a Data Subject, the Data Processor shall respond and inform the Data Subject that request cannot be acted upon because the request has been sent to a Service Provider. In addition, the Data Processor must notify the Data Controller within three [3] working days of such Request.

If the Data Processor considers that an instruction constitutes a violation of the GDPR or of any other Applicable Data Protection Laws, it shall immediately inform the Data Controller.

The Data Processor undertakes to cooperate with the Data Controller to ensure compliance with the obligations regarding the security of Data Controller Personal Data, notification of a Data Breach, communication of the Data Breach to the Data Subjects, implementation of an impact assessment and, where appropriate, prior an audit of the competent supervisory authority.

The Data Processor undertakes to provide the name and contact details of their data protection officer (DPO), or Chief Privacy Officer (CPO) where applicable.

The Data Controller has a duty to fully and effectively, upon demand, indemnify, reimburse, save and hold to the broadest extent allowed by law, the Data Processor, and each of the Data Processor's former, present and future officers, directors, shareholders, lawyers, agents, designees, employees, assignees, successors and assigns ("Affiliate(s)"), harmless from and against any and all third party (including any Supervisor Authority) lawsuits, liabilities, claims, actions, proceedings, demands, judgments, costs, expenses, causes of action, losses, and damages of every kind and nature now or later contemplated (including without limitation, all attorneys' fees and all costs in any manner related to them in whole and in part) ("Claim(s)") incurred or sustained by the Data Processor by reason of the Data Collector's negligence, willful misconduct, or bad faith in connection with the collection and the transfer of the Personal Data to the Data Processor, or an actual, alleged or anticipatory breach or default ("Breach(es)") of this DPA by or on behalf of the data Controller.

The Data Processor will give notice to the Data Controller of any Claims, and the Data Controller has a duty to immediately undertake at its sole cost and expense the defense of that Claim, and supply competent and experienced counsel to the Data Controller satisfactory to the Data Controller in its discretion, to defend that Claim.

8. SUB-PROCESSORS

8.1. Authorized Sub-processors

The Data Controller authorizes the Data Processor to subcontract to Sub-processors any of its Service-related activities and according to the present article. This authorization shall constitute a general written authorization within the meaning of Art. 28 (2) GDPR.

Any Sub-Processor used must qualify as a Service Provider as defined by the CCPA, and the Data Processor cannot make any disclosures to the Sub-Processor that the CCPA would treat as a sale.

The Data Processor currently works with the Sub-processors specified in Annex 2 and the Controller agrees to their appointment.

The Data Processor will inform the Data Controller in advance and in writing of any planned changes concerning the addition or replacement of any Sub-processors. This information must clearly indicate; (i) the Sub-processor' name, address, and contact information; (ii) the type of service provided by the Sub-processor; (iii) the Personal Data categories disclosed to the Sub-processor in the preceding twelve (12) months; and (iv) the dates of the subcontracting contract.

The Data Controller may object to an intended change. The objection to the intended change must be notified to the Data Processor within ten (10) days after receipt of the information on the change. In the event of an objection, the Data Processor may, at its own discretion, either provide the service without the intended change or propose an alternative subcontractor and coordinate it with the Data Controller. If the provision of the service is unreasonable for the Data Processor without the intended change - for example, due to the associated disproportionate costs for the Data Processor - or the agreement on an alternative Sub-processor

fails, the Parties may terminate this DPA as well as the Principal Agreement.

The Data Processor will ensure that the Sub-processor is bound by the same data protection obligations of the Data Processor under this DPA, shall supervise compliance thereof, and must in particular impose on its Sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of EU Data Protection Law.

The Data Processor remains fully liable for the Sub-Processor's performance of its agreement.

8.2. Mobile Measurement Partners

The Parties acknowledge and agree that Data Processor may provide Data Controller Personal Data to Data Controller's mobile measurement partners and that such transfer is due to certain arrangements between Data Controller and its relevant mobile measurement partners. Data Controller's mobile measurement partners are not Data processor's Sub-processors. This DPA does not govern, and Data Processor shall not be liable for, the Processing of Data Controller's Personal Data by Data Controller's mobile measurement partners.

9. INTERNATIONAL TRANSFER OF PERSONAL INFORMATION

9.1 UNDER GDPR

IF the Data Processor is required to transfer Data Controller Personal Data to another country or to an international organization under European Union law or any other law to which it is subject, it must inform the Data Controller prior to the processing, unless the law concerned prohibits such information on important public interest grounds. Such transfer to a third country could take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled.

The Standard Contractual Clauses and the additional terms shall apply to legal entity that is not incorporated under one of the countries recognized by The European Commission as a country that offers an adequate level of data protection. Where the transfer of Personal Data is made subject to the Standard Contractual Clauses, the "Data Importer" thereunder shall be either the Processor or Sub-Processor, as the case may be and as determined by Processor, and the "Data Exporter" shall be the Controller of such Personal Data.

9.2 UNDER PIPA

If Personal Data is transferred outside of the Republic of Korea, the Data Controller must obtain separate consent for the transfer of data, providing detailed information on the destination country, the receiving entity and the Personal Data protection measures in place. The foreign entity must provide a level of data protection comparable to that required in the Republic of Korea. If this level is not deemed sufficient, the Data Controller commits to take steps to guarantee an adequate level of protection, for example, via contractual clauses or agreements.

10. SECURITY

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the Data Controller Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, and comply with any and all security obligations pursuant to the Applicable Data Protection Laws, including, without limitation and as appropriate, the measures referred to in Article 32(1) of the GDPR.

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

The technical and organizational measures implemented by Adikteev to guarantee information system

security are described in the Security Assurance Plan specified in Annex 3.

11. AUDIT

Each Party may – only once a year – carry out or have carried out by any mandated third party of its choice, at its own expense and after giving fifteen (15) working days' notice in writing to the other Party, an audit of the compliance of the collection, transmission and Processing of Personal Data.

The auditor's engagement letter will be transmitted to the Party concerned at least three (3) business days before the start of the mission.

The Parties agree that an audit may be carried out only on condition that the auditors sign a non-disclosure agreement before the start of their assignment.

In the context of such audits, the Party concerned undertakes to cooperate fully with the auditors and to provide them with all necessary information.

In the event that an audit report would reveal a failure to comply with the obligations of the Party concerned, the latter expressly undertakes, at its own expense, to implement all necessary corrective measures within a three (3) months period of time and consistent with any injunction or obligation imposed by a Supervisory authority.

If the conclusions of such audits contain recommendations for modification or improvement of the rules and procedures audited, the implementation of such recommendations shall be carried out by the Party concerned within a period of time to be agreed between the Parties.

The audit may be carried out in the form of a documentary audit and/or interviews and/or an audit of the information systems and applications implemented as part of the Services, including an audit of the code.

12. MISCELLANEOUS

12.1. Inconsistency

In the event of any inconsistency between the provisions of this DPA and the provisions of the Principal Agreement, the provisions of this DPA prevail.

12.2. Limitation of liability

The liability of the Data Processor under this DPA shall be limited to a maximum aggregate amount of one million (1,000,000) euros, regardless of the cause or nature of the claim or action.

12.3. Governing Law and Jurisdiction

The Parties to this DPA submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including but not limited to, disputes regarding its existence, validity or termination or the consequences of its nullity; and (ii) this DPA 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.

12.4. Severance

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA remains valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as close 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.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the Effective Date first set out above.

This agreement may be electronically signed. The Parties agree that any electronic signatures appearing on this agreement are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility.

For and on behalf of the Client	For and on behalf of Adikteev
Signature	Signature
Name:	Name:
Title:	Title:
Date Signed	Date Signed :

ANNEX 1. DETAILS OF THE PROCESSING

NATURE AND DETAILS OF THE PROCESSING

- The creation by the Data Processor of a database allowing the creation of audience segments for the purpose of displaying targeted advertising messages,
- the identification of relevant Users in the context of the real-time bidding system allowing the purchase of advertising space from mobile Applications in order to display the ads as instructed by the Data Controller,
- measuring performance of and optimizing advertising campaigns on behalf of the Data Controller,
- analyzing trends,
- deriving insights,
- developing machine learning models (i.e, prediction tool predicting the users that are about to churn and the users' affinity across a portfolio of the publisher's apps),
- Reporting on advertising campaigns,
- prevent displaying ad to the same user too many times;
- Performing the Principal Agreement, this DPA and/or other contracts executed by the Parties ;
- Generating de-identified and/or aggregated data; improving the Services;
- Developing new products and services;
- Acting upon Client's instructions when consistent with the terms of the Principal Agreement;
- Providing support and technical maintenance, if agreed in the Principal Agreement ;
- Preventing, mitigating and investigating the risks of data security incidents, fraud, error or any illegal or prohibited activity;
- Complying with applicable laws and regulations;
- All tasks related to any of the above.

TYPE OF PERSONAL DATA

- Unique Identification Information (IDFV / IDFA / GAID and other similar unique identifiers)
- Mobile app technical information (OS, device model)
- Behavioral Information (users interactions with an app, scrolls, clicks, opening, add to basket etc.)
- Demographic data (non precise localisation, age, sexe)

DURATION OF THE PROCESSING

Data Retention:

In order to provide the Services, the Data processor shall retain the Data Controller Personal Data provided by the Data Controller for a maximum period of three (3) years following the transfer of the data, provided that when the contractual relationship between the Parties is a succession of "Insertion Orders" linked to the Client's advertising campaigns, if the Client's advertising campaign is paused for over two (2) months, the related Client Personal Data will be archived until the next campaign.

Data Deletion :

At the termination of the Agreement, the Data Processor will, at Data Controller's request, delete all Data Controller Personal Data, except where Data Processor could have to retain copies under applicable laws, in which case Data Processor will isolate and protect Data

Controller Personal Data from any further processing except to the extent required by applicable laws.

Any request for deletion of one or several Data Controller Personal Data must be submitted in accordance with Data Processor's data deletion procedure which can be made available upon request of the Data Controller.

CATEGORIES OF DATA SUBJECT

- mobile apps users

ANNEX 2. AUTHORIZED SUBPROCESSORS

Following is ADIKTEEV's current list of third-party sub-processors who are authorized to process personal data as part of the ADIKTEEV service for the Contracted Business Purpose:

Sub-processor name	Purpose	Locations
ADIKTEEV's Affiliates - **Adikteev Inc** - **Adikteev SA**	Providing the Services	- Adikteev Inc, USA - Adikteev SA, France
Amazon Web Services, Inc. (including its sub-contractors as listed at https://aws.amazon.com/compliance/third-party-access/)	Data Hosting	- European Union - USA - Singapore

1. Definitions

"Customer" means the entity(ies) of the Adikteev company concerned by the Service performed or under discussion with Adikteev.

"Contract" means the contract concluded between the Customer and Adikteev relating to the Services.

"Data" means the Customer's data that may circulate, be generated, collected by any solution used by Adikteev or that would be entrusted to Adikteev by the Customer, in the context of the performance of the Services, including Personal Data.

"Personal Data" means any information relating to a natural person identified or who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, or to one or more elements specific to his physical, physiological, genetic, mental, economic, cultural or social identity.

"Adikteev" means the company Adikteev SA and Adikteev Inc and any company directly or indirectly related to.

"Brand" means the registered trademark "Brand" used to promote and identify the solution(s), tool(s) and offer(s) developed and sold by Adikteev.

"Parties" means simultaneously the Customer and Adikteev.

"SAP" or "Security Assurance Plan" means this security assurance plan, established between the Customer and Adikteev.

"Service(s)" means the service(s) subject to the call for tenders, discussions between the Parties or the Contract, having a direct or indirect link with the Information System, the data.

"Resources" means all hardware and software components including, but not limited to, (i) computer equipment (fixed or portable computers, tablets, mobile or fixed phones, servers, USB devices, network equipment, printers, copiers, scanners,...), (ii) means of communication, storage and exchange of information (Internet, Intranet, messaging, storage, information sharing services, collaboration, on the company's system and in the cloud, ...), and (iii) applications and software.

"IS" means the Customer's information system and/or by extension that of the Customer's service providers or subcontractors in connection with the system.

“Chief technology officer” (**CTO**) is the executive-level position in a company whose occupation is focused on the scientific and technological issues within an organization. CTOs will make decisions for the overarching technology infrastructure that closely align with the organization's goals.

2. Purpose of the Security Assurance Plan

This Security Assurance Plan (SAP) defines the security measures implemented by Adikteev to guarantee information system security in the context of relations between Parties. This document describes the technical and organizational measures implemented to meet the Customer's security requirements in terms of data protection and information system security.

The Service Security Assurance Plan constitutes a reference for the development, management and guarantee of the security of the Service.

The SAP applies to Adikteev and all its employees performing the entire Service.

The SAP is an annex to the contract concluded between the Parties.

3. Services provided by Adikteev

Adikteev delivers personalized and relevant re-engagement mobile advertisements to application end-users and provides the client with reports containing aggregated data on the results of the advertising campaigns carried out.

2 different offers are available:

- **DSP** – Promote the client ads in other apps through account manager and reporting
- **Cross-promo** – Promote clients apps in their own apps through a SaaS solution.

4. SAP Management

Creation of the Security Assurance Plan (SAP)

The SAP is defined by the CTO as part of process documentation. It is distributed to the entire project team working on the Service for application.

Amendment of the SAP

Any modification of the SAP will be the subject of an amendment signed between the Parties.

The SAP must be modified by the CTO as soon as the requirements or measures must evolve throughout the duration of the Service, in particular in the following cases:

- Customer request
- Evolution of the information system (architecture) or its environment.
- Project hazards

- Evolution of risks
- Difficulty or impossibility of applying certain measures.

It is validated by the client.

Application of the SAP

The SAP is applicable to all actors of the Service. The CTO is responsible for the application and monitoring of the SAP.

Derogations from the SAP

In the event of inability to complete one of the SAP measures, Adikteev's CTO makes a request for derogation to the Client to validate the terms of the derogation.

Non-compliance with the SAP

Any stakeholder in the project identifying non-compliance with the SAP must inform Adikteev's CTO via a formal communication by email, specifying:

- The part of the SAP that is subject to non-compliance.
- The security requirement that is not covered.
- The risks generated by this non-compliance.
- The proposed means of treatment (derogation, evolution of the SAP, compensatory measure).

5. Organization of security

Adikteev protects the Customer's Data and services against accidental or unlawful destruction, accidental loss, alteration, dissemination or unauthorized access, as well as against any other form of unlawful processing through its identification and response data breach plan document.

Adikteev is bound by an obligation to advise, warn and recommend in terms of safety and state of the art. As such, Adikteev may inform the Client of the risk of a proposed operation and the associated corrective actions or preventions.

6. Human Resources Management

Before hiring

All stakeholders of Adikteev have a non-disclosure clause in their employment contract. It covers the activities carried out by the latter within the framework of the services provided.

Also, an IT charter has been formalized and sets out within Adikteev the rules relating to the use of these resources.

This charter aims to:

- make users aware of the risks associated with computer security with regard to freedoms and privacy, in particular through the processing of personal data, which they are required to implement;
- inform users about:
    - the authorized uses of the IT resources made available to them by Adikteev;
    - the safety rules in force;
    - the control measures that can be implemented by the IT department in accordance with the applicable regulations;
- formalize the general security rules that Users undertake to respect, in return for the provision of information systems and computer equipment, and thus determine the rights and duties of Users.

The obligations described in this IT charter apply to any person using Adikteev's information systems.

During the contract

Adikteev employees are regularly made aware of data protection and good behavior in terms of cybersecurity, including raising awareness of the threats relating to the misuse and non-compliance with the basic rules of information security and the protection of privacy, in relation to the daily use of the IT resources made available to them, via, for example, phishing simulations.

Adikteev makes its various stakeholders aware of IT security in general and more particularly of the security obligations related to the Service.

Adikteev also has a complete and up-to-date directory of all its employees and subcontractors involved or having intervened in the context of the Service. This directory specifies the roles and responsibilities of each stakeholder, their scope of intervention, date of arrival on the Service and date of departure of the Service if applicable.

Adikteev ensures compliance, by its employees working on the IS, with the laws, regulations and the Security Insurance Plan in force.

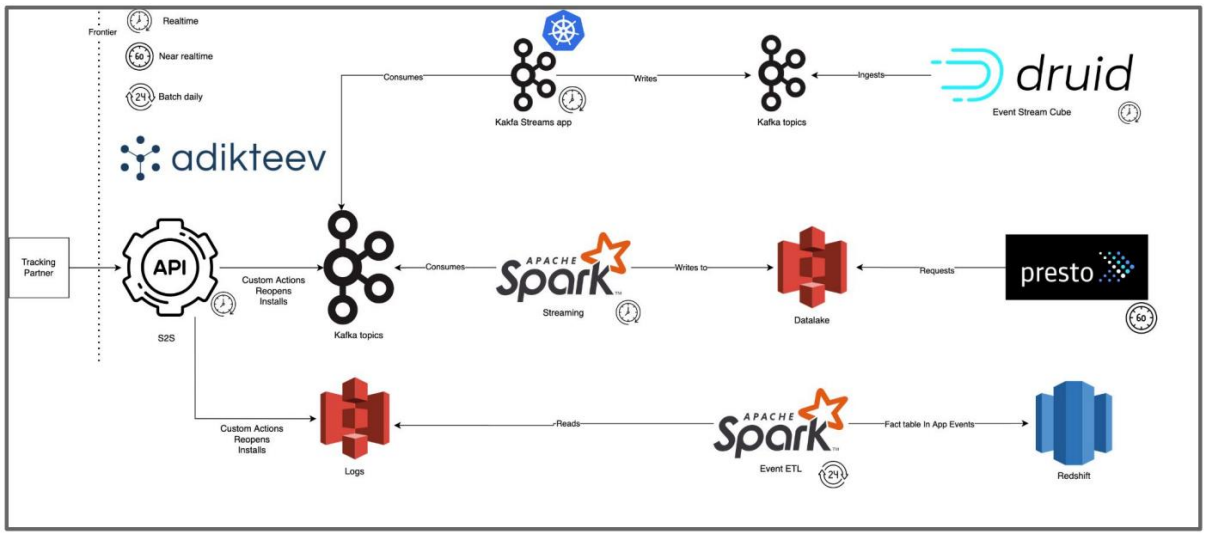
At the end or in the event of modification of the contract

When an employee leaves, a formal procedure ensures that all property is returned, in accordance with the procedure.

Accesses to the IS are also checked and if necessary, deactivated.

7. Management of technical resources

Cartography



Adikteev has an up-to-date mapping of the Resources used in the context of the Service.

Adikteev undertakes that all parties involved in the Service only use Protected Resources in accordance with the state of the art, particularly in terms of dataflow encryption and data protection.

Classification of information

At the start of the Service, Adikteev will agree with the Customer on the level of confidentiality and criticality of the information processed, this classification serving as a basis for determining the means of protection (storage, data lifecycle, backup) to be implemented through its Data Processing Agreement document.

By default, the following data is considered sensitive and to be protected:

- Mobile advertising identifier (GAID/IDFA)
- User operations within an app (e.g. in-app purchases)
- Information about the advertisements that users have seen or clicked on
- Some metadata, such as timestamp, device type and model, app and its version, country

Information Protection

Any document or information considered confidential or critical is subject to the following protection:

- encryption of the Data transmission in accordance with the state of the art, during exchanges between the various actors of the Service.
- secure storage and organizational measures to restrict access only to authorized persons and prevent disclosure, accidental or unlawful destruction, accidental loss or alteration.

At the end of the Service, Adikteev asks the Customer to follow up on the information in his possession: the destruction or retention of the information. By default, sensitive customer data is retained for up to 91 days. In case of retention, all follow-up documents and data will be automatically deleted after 1 year.

Data can be deleted in the event of a customer request, end of the contract or when a user has withdrawn his consent. No copy of the information circulates outside the infrastructures and offices of Adikteev.

Adikteev implements the necessary security measures to comply with regulatory requirements related to Personal Data especially regarding:

- the French & European GDPR standard
- the US Californian CCPA standard

Adikteev guarantees the preservation of the archives in conditions ensuring their protection, durability and legibility.

Scrapping

Before any maintenance operation outside Adikteev's premises, at the end of the use of a material (sale, reallocation or recycling), the hard disks of the workstations used as part of the Service, are securely deleted.

8. Logical access management

Authorization Management

Adikteev is responsible for the management of access accounts to the Resources. All access and associated authorizations are nominative and non-transferable (no generic accounts).

Adikteev establishes, maintains and regularly reviews the authorizations on its resources by guaranteeing an appropriate separation of tasks and incompatible areas of responsibility on the principle of least privilege. In the event of a change of responsibility or internal transfer of an employee, Adikteev updates the authorizations concerned.

In the event of the departure of an employee, his account is deleted within a reasonable time and compatible with the operation.

Account and password management

Each user authenticates himself by a unique identifier and a password whose complexity is defined by Adikteev, in proportion to the criticality of the information processed. Accounts are personal and passwords confidential.

Technical account credentials are protected through the dedicated secret management solution Vault.

Adikteev implementation relies on three main SSO providers:

- Google Workspace
- Github
- Amazon IAM

For these three providers, a double factor authentication is pushed.

Traceability of user access

Adikteev keeps all traces of access and modifications made to the authorizations.

9. Physical Security

Physical access control to premises

Access to the premises used as part of the Service is controlled biometrically or by badge. The management of the systems used is under the responsibility of Adikteev.

Adikteev does not have any physical server on its premises.

Traceability of physical access to premises

Adikteev maintains the list of all authorizations to the physical access of its employees and the nominative list of external personnel to the company likely to intervene in the areas used for the Service.

Adikteev has the means to verify at any time the authorizations of the staff accessing its premises.

Protection of premises

The buildings and premises used by Adikteev have detection/protection systems against fire. These systems are operational on a permanent basis (24/7).

All premises used by Adikteev for the Service are equipped with intrusion detection systems (door alarms etc.), permanently operational (24/7).

10. Information System operations

Procedure

The main Operations procedures of the IS are documented, kept up to date, and available even in the event of a disaster.

An IS map is formalized, kept up to date, and available even in the event of a disaster, to describe the IT system, its architecture and the sensitive points.

Server infrastructure

Servers and infrastructure components are installed in an Amazon AWS infrastructure and therefore benefit from all the Amazon supplier's security features. The infrastructure and its hosting are subcontracted, this subcontracting is the subject of a proper contract and service level guarantees.

In the event of pooling of infrastructures, Adikteev implements appropriate measures to avoid logical access by unauthorized third parties.

Backups and restores

Adikteev ensures a full backup of information and software through Amazon backup services. Adikteev regularly performs recovery tests to ensure the reliability of the backups made.

As Adikteev wishes to guarantee the quality of service of the operations carried out in its Amazon AWS infrastructure to its customers as well as to the company employees, it has formalized a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

Traceability of operations

The actions performed on the Data are plotted on different levels of criticality as detailed as possible.

The generated traces are centralized and monitored in Grafana or in a dedicated Amazon AWS solution ensuring the integrity and availability of the logs. Any trace showing an anomaly is analyzed and processed by a dedicated team in a monthly technical committee.

Security Patch Management

Adikteev respects the recommendations of manufacturers and publishers concerning the maintenance of the Resources.

A vulnerability detection process is in place for all delivery resources. Any discovery of a critical flaw shall be notified without delay. Critical security updates are deployed as soon as possible after they are released.

When no fix is available, Adikteev follows the recommendations of the manufacturers and/or publishers as part of a temporary circumvention and keeps the Customer informed of the current action plans.

Fight against malicious code

Software to combat malicious code (viruses, Trojan horses, worms, spyware, etc.) is activated and kept up to date on workstations and servers linked to the Service. Adikteev has also deployed an XDR to monitor the security of it Cloud infrastructure.

Alerts are analyzed and processed as soon as possible.

Vulnerability Management

The systems and software used are in versions supported by the editors or, where applicable, by the community.

The systems and software are kept up to date on a regular basis, after validation of the security patches by tests of proper functioning and non-regression on test equipment.

Security audit

Adikteev regularly has security audits (penetration test) carried out on the solutions made available to its customers. The resulting action plans are processed according to the criticality of any reported vulnerabilities.

Incident detection and management

Detection procedures for managing security alerts/incidents are in place to deal with any event that may affect the security of the Service or the IS. Adikteev will immediately inform the Customer of any security incident of which it may have become aware, including in particular data breaches.

This information, which will be updated throughout the resolution of the incident, will include at least:

- A detailed description of the facts found
- An assessment of the risks associated with the incident
- The precautionary measures put in place
- The proposed action plan

Crisis management

A crisis management process is formalized, kept up to date and tested regularly.

11. Data exchange

Network Security

The production networks used as part of the Service are partitioned from Adikteev's other networks. The resources made available by Adikteev are subject to control for incoming and outgoing access.

Adikteev's production networks must only accommodate Material Resources controlled by the latter.

Securing Data Transmissions

Adikteev's networks used as part of the Service are secured by encryption and password and guarantee the confidentiality and integrity of the flows.

Control of the solutions used

As part of the Services, Adikteev ensures that the solutions it uses, and the associated license agreements, preserve the ownership and integrity of the Data.

Remote access to IS

Adikteev may authorize its employees to work remotely provided that the workstations are mastered and use a VPN secured by strong authentication.

12. Security of control, reporting and audit developments

Development rules

Adikteev integrates security best practices into any development, in particular:

- those recommended by the OWASP (Open Web Application Security Program)
- those concerning systematic peer review

Adikteev also uses a Static Application Security Testing (SAST) solution, in order to supervise the security of its developments.

Compartmentalization of environments

Developments are carried out in a dedicated environment, separate from the production environment and without connection to it. No developer account has production access.

Testing is performed with test datasets and in no case with production data. If these test datasets are generated from the Actual Data, they are distorted to make them completely anonymous.

Development Management

Adikteev ensures that developers are trained in secure development techniques. The company ensures secure change management: no deployment in production is carried out without prior testing and informing the Customer of potential operational impacts.

Each deployment of a new version of the solution includes the latest security patches (systems, applications, etc.). Adikteev implements practices of deletion or deactivation of unused or obsolete services.

Retention of information

The developments are carried out in such a way as to expose personal information to a minimum thanks to a secret management solution such as Vault.

13. Partners and subcontractors

Adikteev undertakes to have signed with each partner one:

- Non-disclosure Agreement
- Data processing Agreement
- Contract

Adikteev also undertakes to check that the intervention of third parties (for maintenance or repair) is the subject of formalized procedures and that these make it possible to protect the data entrusted to the host.

Control, reporting and audit

Adikteev ensures a permanent control of the IT security of the activities for which it is responsible, including with its own subcontractors.

Adikteev must provide, at the Customer's request any document, report, certification allowing it to demonstrate its compliance with the security requirements resulting from this SAP and the Contract.