PURCHASELY'S DATA PROCESSING AGREEMENT

Updated : July 8th 2024, version 5

PRELIMINARY REMARKS

The purpose of this document is to define the Processing operations and Personal Data Processing accomplished by the Supplier on behalf of the Client in the context of the provision of Services as defined in the Terms of services.

This Data Processing Agreement aims to ensure that the Parties respect the Personal Data Regulations and to establish guarantees and procedures for the lawful Processing of Personal Data.

It is an integral part of the Agreement together with the Terms of services and the Contractual Undertaking signed by the Client and the Supplier.

Article 1. DEFINITIONS

Unless otherwise defined in the Agreement, all the terms in the upper case used herein, including the Preliminaries, shall have the meaning given in Purchasely's Terms of services, or, failing that, as follows:

- **Agreement** shall mean the Terms of services, the Contractual Undertaking signed by the Client and the Supplier and this Data Processing Agreement;
- **Data Controller,** according to Art. 4, paragraph 7 of the GDPR shall mean the organ which, alone or with other directors, shall decide on the purpose and terms of the Personal Data processing;
- **Data Subjects' Rights** shall mean the Data Subjects' rights by virtue of the Personal Data Regulations;
- **EEA** shall mean the European Economic Area;
- **Personal Data** shall mean personal data within the meaning of the Personal Data Regulations;
- **Personal Data Breach** shall mean a security breach resulting, accidentally or unlawfully, in the destruction, loss, alteration, unauthorized disclosure of Personal Data;
- **Personal Data Regulations** shall mean the Law no. 78-17 dated January 6, 1978 relating to I.T., files and liberties (Data Protection Act) and the General Data Protection Regulations (called "**GDPR**") dated April 27, 2016 published in the Official Journal of the European Union on May 4, 2016 relating to the protection of individuals with regard to personal data processing and the free movement of this data, and any regulations which shall apply for personal data protection, in particular the EC Directive 2002/58 by the European Parliament and Council dated July 12, 2002 concerning the processing of personal data and privacy protection in the electronic communications sector (referred to as the "**Privacy and electronic communications directive**" or "**E-privacy directive**") and any new regulation which shall replace such Directive;
- **Processing or Process** shall mean, within the meaning of the Personal Data Regulations, any operation or set of operations, whether or not carried out with the assistance of automated processes and applied to Personal Data, such as the collection, registration, organization, structuration, retention, adaptation or modification, extraction, consultation, utilization, communication by transfer, dissemination or any other form of availability, the reconciliation, interconnection, limitation, deletion or destruction;
- **(Purchasely's) Data Processing Agreement** shall mean this contractual document, with the purpose of defining the conditions and terms of enforcement of the Personal Data processing operations, made in the context hereof;
- **Purchasely ISSMP** shall mean the documentation, defines the organizational and technical security rules setup by the Supplier. This documentation may be

modified at any time (without substantively calling into question the level of security), without notice, by the Supplier depending, in particular, on the Service developments. The duly modified documentation shall automatically apply upon notification sent by the Supplier to the Client. This documentation is at the Client's disposal upon his request by email;

- **Services** shall mean the services provided by the Supplier to the Client, as agreed herein;
- **Sub-contractor or Data Processor** according to Art. 4, paragraph 8 of the GDPR shall mean the individual or legal entity, public authority, service or any other body which processes Personal Data on behalf of the data controller;
- **Subsequent Sub-contractor** shall mean an entity hired by the Sub-contractor to assist with (or which accomplishes) the Personal Data Processing for the Data Controller in the context of the Sub-contractor's obligations in accordance with the Agreement, such as mentioned in the Data Processing Register attached hereto;
- **Sensitive Personal Data** according to Art. 9 of the GDPR shall mean Personal Data revealing the data subjects' alleged racial or ethnic origin, the political opinions, religious or philosophical convictions or the trade union membership, genetic and biometric Personal Data, Personal Data concerning data subjects' health, sexual activity or sexual orientation, Personal Data relating to the criminal convictions or offenses, and the unique national identification number (NIR or social security number);
- **Supervisory Authority** shall mean any authority authorized to control and ensure the respect of the application of the Personal Data Regulations concerning the Personal Data Processing accomplished in the context of the Agreement and the provision of Services.

Article 2. GENERAL STIPULATIONS AND DEFINITION OF ROLES

The performance of the Agreement shall result in the Personal Data Processing by the Parties in order both for the management of the commercial relations between the Parties and the provision of Services for the Client's benefit.

Such Processing is subject to the Personal Data Regulations. The Parties declare to be aware of each of their respective rights and obligations, resulting from the application of the Personal Data Regulations to the Personal Data Processing setup in the context of the performance hereof.

The Supplier and the Client shall undertake to collect, process, use and transfer the Personal Data within the respect of the Personal Data Regulations.

They undertake to process the Personal Data loyally and legally in all circumstances.

They declare to have respected all their statutory obligations in this regard and undertake to respect them for the entire duration hereof, and, in particular, to proceed

with any declaration with the Supervisory Authorities or that of the Data Subjects and/or obtain from such authorities and the Data Subjects any authorization necessary, in the context of the collection and Processing of the Personal Data for the purpose of the Services provided herein.

The Parties acknowledge to have been fully informed of the Personal Data Regulations obligations which apply in their regard in their respective capacity of:

- **Independent Data Controllers for the Supplier and the Client** concerning their respective Personal Data Processing in order to manage their commercial relations;
- **Data Controller for the Client and Sub-Contractor for the Supplier** concerning the Personal Data Processing carried out in the context of the provision of Services, i.e., the Processing related (i) to the purchasing of a product or a digital subscription by the Users and (ii) the technical and operational provision of Services, in particular, with the view to the use and/or management on its behalf of the Identifiers enabling the Contacts to access its Internet platform.

Article 3. SUB-CONTRACTING OF THE PROCESSING CARRIED OUT BY THE SUPPLIER

Concerning the Personal Data Processing accomplished in the context of the provision of Services:

- the Supplier acts in the capacity as Sub-Contractor;
- the Client acts in the capacity as Data Controller.

3.1. The Sub-contractor's obligations

In the context of the provision of Services, the Supplier, in his capacity as Sub-Contractor shall undertake to respect the following obligations and ensure that they are respected by his personnel:

- provide the Data Controller with sufficient guarantees for the setup of the appropriate technical and organizational measures, in terms of the formation of the Sub-contractor’s personnel members assigned to the Services, the equipment used, to ensure that the Personal Data processing setup for the purpose of the performance of the Agreement meets the requirements under the Personal Data Regulations;
- only to process Personal Data upon the duly documented instruction of the Data Controller, it being specified that if the Sub-contractor considers that an instruction / a Processing from the Data Controller constitutes a breach of the Personal Data Regulations, he shall inform the Data Controller as soon as possible and he can ask the Data Controller to demonstrate that its instruction /

Processing does not constitutes a breach of the Personal Data Regulations and/or the Agreement and meanwhile he can refuse to apply this instruction / Processing ;

- process the Personal Data only for the purpose provided by the Agreement, with the exception of subsequent Processing of anonymized data exclusively carried out for the purpose of statistics and research for the continuous improvement of the Services, for which the Data Controller acknowledges the Sub-Contractor's legitimate interest for the implementation thereof;
- ensure that the persons authorized to process the personal data undertake to respect the confidentiality or are subject to an appropriate statutory confidentiality obligation;
- guarantee the security of the Sub-contractor's premises, to prevent the destruction, loss, alteration, distortion or other modification, hacking, misappropriation, damage, disclosure or access to the Personal Data by unauthorized persons for which the Sub-contractor has been communicated, stored by the Sub-contractor or, more generally, that he processes in any means whatsoever, on behalf of the Data Controller;
- cooperate with the Data Controller, in particular, by providing him with the necessary documentation to establish the respect of all his obligations, in particular, the realization of audits (according to the terms of Article 3.13), including inspections, by the Data Controller or another auditor, independent and non-competitor of the Sub-contractor, mandated to contribute to these audits;
- have respected all the Sub-contractor's obligations under the Agreement by any substituting company or its *modus operandi*, by expressly providing these same obligations for the Sub-contractor, and any Subsequent Sub-contractor, regardless of his rank in the agreement between the Sub-contractor with the company or any subsequent Sub-contractor, to ensure their respect of the Agreement;
- notify the Data Controller, under the conditions of the Personal Data Regulations and in accordance with Article 3.12 below, of any Personal Data Breach of which the Sub-contractor would have been made aware thereof, take the appropriate measures as soon as possible to remedy this situation, including any appropriate procedure before the competent Supervisory Authority and cooperate with the Data Controller to communicate by mutual agreement on the existence of the Personal Data Breach with the data subjects.

3.2. The Data Controller's obligations

The Data Controller shall undertake to provide to the Sub-contractor all the necessary information and elements enabling the latter to perform the Agreement and provide the Services in accordance with the Agreement, and those enabling the Sub-contractor to respect its own obligations in terms of personal data protection.

In the event whereby the Data Controller were also to provide Data to the Sub-contractor, directly or indirectly, he shall ensure that the latter is accurate, relevant,

appropriate and limited to that strictly necessary with regard to the Processing objectives.

The Data Controller shall undertake to document in writing any instruction concerning the Data Processing by the Sub-contractor.

The Data Controller shall also be responsible and shall undertake as follows:

- to ensure the lawful, loyal and transparent collection and Processing of the Data;
- to provide the information necessary to the data subjects and ensure, in the event whereby consent is required, that the latter had been duly obtained, i.e., explicitly issued for each purpose, and that it is able to be tracked and withdrawn at any time by the data subjects. In this regard, and if the Sub-contractor is in charge of accomplishing operations for the collection or Processing on behalf of the Data Controller, the latter shall communicate to the Sub-contractor any mention of information or acquisition of consent and any complementary instruction to be issued to the data subjects;
- ensure that the Personal Data is only collected and processed for a specific, explicit and legitimate purpose and that it is adequate, relevant, non-excessive and limited as required with regard to the intended purpose;
- ensure the quality, accuracy and update of the Personal Data;
- where a Processing of Sensitive Personal Data setup by the Controller through the Services happens, ensure that such Processing complies with Art. 9, paragraph 2 of the GDPR ;
- where a Processing of Personal Data of an individual under the age of 13 (children) setup by the Controller through the Services happens, ensure that such Processing complies with Personal Data Regulations but also complies with the US Children's Online Privacy Protection Act (COPPA), it being specified that, through the Services, children's personal data is not saved, nor exploited commercially, only processed on behalf of the Client for Processing no. 3 according to the Purchasely's Processing Register : All the operation enabling the customization of the User journey and of the commercial offers presented ;
- ensure that the Personal Data is not kept beyond the duration necessary with regard to its required purpose. In this regard, the Data Controller shall define and communicate to the Sub-contractor the retention periods to be applied to the Personal Data processed by the Sub-contractor in the context of the Agreement; Data Controller is informed that the Personal Data are kept by the Sub-contractor, by default for a specific retention period (cf. the Purchasely's Processing Register) but Data Controller can set up a different Personal Data retention period ;
- to ensure the respect of the data subjects' rights (in particular, the right of access, interrogation, rectification, objection, deletion, limitation, portability) and to respond to the data subjects' requests according to the terms and within the periods required.

The Data Controller shall hold harmless the Sub-contractor for any complaint arising from the Data Subjects to the extent the complaint is arising out of Data Controller's breach of the applicable law.

The Sub-contractor shall hold harmless the Data Controller for any complaint arising from the Data Subjects if arising out of Sub-contractor's breach of the applicable law or security measures.

3.3. Consent to subsequent sub-contracting

The Data Controller acknowledges, accepts and consents that, for the sole exclusive purpose of the provision of Services and subject to the respect of the terms hereof, the Data Controller's Personal Data may be processed by the Sub-contractor or its Subsequent Sub-contractors, the list of which is included in Purchasely's Processing Register.

The Sub-contractor has a general authorization to hire Subsequent Sub-contractors subject to the Sub-contractor: providing the Data Controller with prior information on the Subsequent Sub-contractors' identity and informing the Data Controller of any update of the list of Subsequent Sub-contractors in order for the Data Controller to object to the hiring of these Subsequent Sub-contractors.

In the event of change, deletion or new Subsequent Sub-contractor intervening on the Processing, the Sub-contractor shall notify the Data Controller of the updated list of Subsequent Sub-contractors in writing at least fifteen (15) days before the launch date of the Subsequent Sub-contractor's services. This notification must specifically mention the Processing activities sub-contracted, the identity and contact details of the subsequent Sub-contractor and the dates of the sub-contracting Agreement.

The Data Controller shall have a period of ten (10) days as from the date of receipt of this notification to formulate a written, reasonable and substantiated objection to this modification of the list of Subsequent Sub-contractors.
The Sub-contractor shall take reasonable steps to address the objections raised by Data Controller (for example to present a new Subsequent Sub-Contractor and/or present a modification of Services) and provide to the Data Controller a reasonable written explanation of the steps taken to account for any such objections.

In the event of change, deletion or new Subsequent Sub-contractor intervening on the Processing, the Sub-contractor shall notify the Data Controller of the updated list of Subsequent Sub-contractors in writing at least fifteen (15) days before the launch date of the Subsequent Sub-contractor's services. This notification must specifically mention the Processing activities sub-contracted, the identity and contact details of the subsequent Sub-contractor and the dates of the sub-contracting Agreement.

The Data Controller shall have a period of ten (10) days as from the date of receipt of this notification to formulate a written, reasonable and substantiated objection to this

modification of the list of Subsequent Sub-contractors.

The Sub-contractor shall take reasonable steps to address the objections raised by Data Controller (for example to present a new Subsequent Sub-Contractor and/or present a modification of Services) and provide to the Data Controller a reasonable written explanation of the steps taken to account for any such objections.

The Sub-Contractor shall not appoint, or disclose any Personal Data to, that proposed sub-Processor until reasonable steps have been taken to address the objections raised by the Data Controller.

The Sub-contractor shall undertake to enter into agreements with the Subsequent Sub-contractors including the same obligations concerning the Processing as this Agreement. The Sub-contractor also undertakes to have recourse to SubsequentSub-contractors who present sufficient guarantees, in accordance with those provided under the Agreement, in particular when the latter are applied for setting up appropriate technical and organizational measures for the Personal Data Processing, established in accordance hereto. The Supplier shall stand as guarantor for the respect thereof by any Sub-contractors.

The Sub-contractor shall undertake to accomplish an appropriate and reasonable diligence in the selection of Subsequent Sub-contractors and when the Subsequent Sub-contractors fail to comply with their obligations with regard to Personal Data protection, the Sub-contractor shall remain fully liable for the respect of the obligations stipulated herein by the Subsequent Sub-contractors.

3.4. Security measures

Given the status, costs of implementation and type, scope, context and purpose of the Processing, and the risks, the level of probability and gravity of which varies depending on the rights and liberties of individuals, the Sub-contractor shall undertake to implement the appropriate technical and organizational measures in order to guarantee a level of security adapted to the risk.

The Sub-contractor' technical security measures are detailed in the Purchasely ISSMP, available upon request by the Client.

The Sub-contractor shall undertake to continue these measures throughout the performance of the Agreement. In the event of a change of resources to ensure the Data security, the Provider shall undertake to replace the latter by a performance at least equivalent thereto.

It is understood that the Sub-contractor's commitment resides in the implementation of such measures and not for the accomplishment of a result resulting from such implementation.

3.5. Privacy by design / by default procedure

The Sub-contractor must take the appropriate technical and organizational measures:

- intended to effectively implement the minimization and retention principles for the Personal Data,
- enabling it to be ensured that, by default, only the Client's Personal Data for each specific Processing objective shall be processed, including the implementation of archiving and anonymization procedures.

The Sub-contractor uses inter-operable formats to enable the portability of the Client's Personal Data required by the Personal Data Regulations, and setup the organizational and technical measures enabling the Client to duly respect the Data Subjects' rights, in particular the right to access their Personal Data, the right to obtain the rectification or deletion of their Personal Data or the blockage for the Processing of their Personal Data, the right to contest the decisions based on the profiling, and the right of portability for the Personal Data, if applicable.

3.6. Data protection impact assessment

The Sub-contractor assists the Data Controller for the realization of Data protection impact assessment relating to Data protection if the latter is rendered obligatory by the applicable Regulations, given the nature of the Processing and information at theSub-contractor's disposal.

Similarly, the Sub-contractor shall assist the Data Controller for the realization of the prior consultation of the Supervisory Authorities provided under Article 36 of the GDPR.

3.7. International transfers

Unless specifically and expressly authorized to the contrary by the Client, the Sub-contractor shall undertake to process the Personal Data exclusively on the territory of a member State of the EEA.

The Sub-contractor shall undertake not to disclose, render accessible or transfer any of the Client's Personal Data, even for the purposes of data flow, to any Processing entity or any Subsequent Sub-contractor in a third-party country located outside of the EEA, unless the Client has provided prior written consent.

In the event of a transfer outside of the EEA authorized by the Client, such transfer shall only be made as required for the provision of the Services, and insofar as this transfer is operated to a State for which the Personal Data protection legislation was recognized by the European Commission as presenting an equivalent level of protection, or established by the conclusion of standard contractual clauses issued by the European

Commission or carried out on the basis of any other alternative basis recognized by the Personal Data Regulations, subject to the Client's prior written approval on this alternative basis. The Provider shall stand as guarantor for the signature and respect of the requirements herein by its own Subsequent Sub-contractors.

3.8. Cooperation obligations

The Parties cooperate in good faith to ensure the respect of the provisions herein, including, but not exhaustively, to ensure the correct and appropriate exercise of Data Subjects' Rights, manage incidents in the event of a Personal Data Breach in order to mitigate any undesirable effects.

The Parties cooperate in good faith to make available to the other Party and the Supervisory Authorities, following a control by the Data Controller, the information required to establish the respect of the Personal Data Regulations.

3.9. Processing registers

The Sub-contractor shall keep a Data Processing Register of the Processing activities accomplished on behalf of the Data Controller, including those granted to its Subsequent

Sub-contractors to whom it has granted all or part of the Processing with the Data Controller's authorization, by mentioning for each Subsequent Sub-contractor the Processing activities granted, the service location, and the Data Controller's Personal Data transfers outside of the EEA and/or outside of the country in which the Data Controller is established or in which the Data Controller's Personal Data is collected.

This register must also include the information concerning the implementation of the appropriate protection measures to ensure an adequate level of protection, such as provided by the Personal Data Regulations.

This register, attached hereto, is accessible at any time for the Data Controller and the Supervisory Authorities.

3.10. Data subjects' rights

Right of information

The Data Controller confirms that he proceeded with all the obligations required with regard to the Personal Data Regulations, and that he had informed the Data Subjects of the use made of such Personal Data.

Processing of the requests for the exercise of Data Subjects' right

The Data Controller shall remain liable for the response to solicitations and requests for the exercise of the Data Subjects' rights.

The Sub-contractor shall provide the Data Controller with reasonable cooperation and assistance and any information reasonably required to respond to the Data Subjects or otherwise, in order to enable the Data Controller to meet its obligations by virtue of the Personal Data Regulations in relation with the Data Subject's Rights.

The Sub-contractor shall make technically reasonable efforts to ensure the interoperability of Personal Data in order for the Data Subjects to exercise their portability right under the conditions provided by the Personal Data Protection Regulations.

The Sub-contractor shall undertake to notify the Data Controller in writing, within a maximum period of seventy-two (72) hours, as soon as he receives a direct request from a Data Subject. The Sub-contractor shall undertake not to respond to any request from a Data Subject without the Data Controller's prior written consent, except for confirmation that the request duly relates to the Data Controller, which the latter hereby accepts.

3.11. The use of the personal data

Upon the termination of the Agreement, the Sub-contractor shall undertake to return and/or destroy the Personal Data under the conditions defined hereafter, at the Data Controller's discretion but the Sub-contractor can keep the Personal Data five more years as intermediate archiving to keep the proof of a right or an obligation of the Agreement

The Sub-contractor shall return or destroy the Data Controller's Personal Data, without expense for the Data Controller, upon the latter's request and upon the expiry or premature termination of the Agreement subject to a written request by the Data Controller, in consideration for a reasonable notice period, unless the applicable mandatory laws (including, but non-exhaustively, the Personal Data Regulations or the authorities in charge of the application of the law), including, but not exclusively, the Supervisory Authority, prevent the Sub-contractor from doing so.

Concerning the Data Controller's specific requests concerning the return of the Data Controller's Personal Data, such a request shall be satisfied without an unjustified delay and at the latest fifteen (15) business days after the Data Controller's request.

If the Data Controller decides to delete the Personal Data, the Sub-contractor shall provide a declaration to ensure such deletion.

3.12. Personal data breach

The Data Controller acknowledges and accepts that the Sub-contractor shall not be held liable for Personal Data Breaches that are not attributable to the Sub-contractor's negligence.

If the Sub-contractor of the data becomes aware of a Personal Data Breach, he shall do as follows:

- take the appropriate measures to limit and mitigate such Personal Data Breach, in particular, by notifying the Data Controller as soon as possible, but under no circumstances more than twenty-four (24) hours after the Sub-contractor has become aware of this Personal Data Breach, to enable the Data Controller to promptly setup his program accordingly;
- cooperate with the Data Controller to define the following: the type, categories and approximate number of Data Subjects, the categories and the approximate number of registrations of Personal Data made and the potential consequences of such Personal Data Breach in order for the latter to be proportionate to its gravity and global impact on the Data Controller and the service provision herein;

When the Personal Data Regulations and/or any applicable regulation requires a notification to the competent Supervisory Authorities and the Data Subjects involved, and insofar as the latter concerns the Data Controller's Personal Data, the Sub-contractor shall defer the latter and take the instructions from the Data Controller who, in its official capacity, is exclusively entitled to define the measures to be taken to comply with the Personal Data Regulations or to remedy any risk, including, but not exhaustively:

- if a notification must be provided to any person, Regulatory body or statutory application body, consumption information agency or other, such as required by the Personal Data Regulations, or at the Data Controller's discretion; and
- the content of this notification, if corrective measures may be offered to the Data Subjects' relevant Data Controller and the type and extent of these corrective measures.

3.13. Audit

In accordance with the Personal Data Regulations, the Sub-contractor accepts the realization of an audit per calendar year, unless expressly requested by a Supervisory Authority, an independent third party auditor, and subject to a notice period notified by registered letter with acknowledgment of receipt at least one month prior to the envisaged date for the audit, to verify the respect of the Personal Data Regulations by the Sub-contractor, under the conditions provided herein.

In this regard, the Sub-contractor shall undertake to assist the independent third party auditor by sending, upon the latter's written request, within due time periods, with regard

to the relevant request, the certifications and/or the most recent summary audit reports that the Sub-contractor has regularly had carried out to verify the effectiveness of the technical and organizational measures.

The Sub-contractor shall cooperate with the independent third party auditor by providing the latter with the complementary information required to ensure the Data Controller's respect of his obligations with regard to audits or to respond to a request by the Personal Data protection Supervisory Authority.

In the context of the realization of these audits by the third party independent auditor, the Sub-contractor shall undertake to assist and respond to the latter's reasonable requests and request the same assistance and response from Subsequent Sub-contractors.

These audits, requested by the Data Controller shall be integrally carried out at the Data Controller's expense- Each party shall assume the internal costs that may be incurred by a Party in connection with such audit;

The independent third party auditor shall not carry out a competitor activity to that of the Sub-contractor and/or have direct or indirect financial relations with a company exercising a competitor activity to that of the Sub-contractor. The Data Controller shall ensure the sincerity and independence of the persons mandated to realize the audit operations. These persons shall be obliged by a confidentiality commitment at least as stringent as the commitment provided herein and concerning all the elements audited, and the subsequent audit report, and more generally, the most absolute confidentiality for the elements which he may have been informed in the context of these audit operations.

It is expressly agreed that the following shall be excluded from the audit: any data, in particular financial or personal data which does not concern the Data Controller, any information, the disclosure of which could affect the security of the Sub-contractor's systems and/or data (in particular, in the event of the risk for the confidentiality of the information) or other of the Sub-contractor's Data Controllers, or the I.T. source code programs used in the context of the provision of the Services.

The duration of the audit shall not exceed three (3) business days. It should be carried out during the Sub-contractor's business hours and shall be conducted in order not to affect the realization of the Services or any other activity carried out by the Sub-contractor.

The Sub-contractor may suspend these audit operations at any time if the realization of the Services or any other of the Sub-contractor's activity requires that the resources and/or means used for the audit be mobilized for other purposes.

The person in charge of the audit operations shall not take any copies of any documents, files, data or information, in full or in part, or take photos, digitalize, or take sound recordings, videos or I.T. screen shots. The person carrying out the audit may also not request that all or part of these elements be provided or sent. The

Sub-contractor may organize a display of sensitive documents in a secured room (black room).

Any person in charge of the audit operations shall only be accepted on the Sub-contractor's site or that of Subsequent Sub-contractors after declaration of his identity by the Data Controller at the time of the notification of this audit in the periods recalled above.

A copy of the audit report shall be issued by the third party auditor mandated simultaneously to the Data Controller and Sub-contractor, who shall meet within a period of fifteen business days in order to study the diligence that should be carried out following the realization of this audit.

3.14. Data protection officer

The Sub-contractor shall communicate to the Data Controller the name and contact details of his data protection officer, if he has made such designation in accordance with the Personal Data Regulations. Reciprocally, the Data Controller shall undertake to communicate to the Sub-contractor the name and contact details of his data protection officer.

DATA PROCESSING REGISTER

Introduction

The Supplier's mission is to provide a simple solution to be implemented, to enable the editors of mobile applications to monetize their application by using the purchasing possibilities and subscription opportunities proposed by the different mobile app stores. The Services enable the Users of the integrated Applications, to make purchases or subscription requests (renewable or not), by using the applications store associated with their smartphone as a means of payment. In order to accomplish this mission, Purchasely shall realize the Processing 4 times, which shall be detailed herein, and for which certain concern Personal Data.

The Data Controller is the Client. The Supplier is his Sub-contractor. This document constitutes the detailed Data Processing Register of Processing.

The Data Controller shall ensure the lawfulness of the Processing sub-contracted to the Supplier. In particular, the Data Controller is responsible for informing the User of the Processing carried out by the Supplier (Sub-contractor). The Data Controller shall be responsible, as the case may be, for obtaining the Users' consent and accomplishing the legal formalities required by a Data Controller for sensitive Personal Data (Privacy Impact Assessment, CNIL declaration etc.). The Supplier, as Sub-contractor, did not carry out a comprehensive Privacy Impact Assessment (PIA). The Supplier's data protection officer shall be available for the Data Controller to assist the latter with the realization of the PIA.

The security measures related to the Processing realized by the Supplier are not explained herein. They are detailed in Purchasely's ISSMP, available upon request by email.

Record of all categories of Processing activities carried out by the Supplier on behalf of the Client

Processing	Processing designation
Processing 1	All the operations which enable the Services to be managed technically and operationally

Processing 2	All the operations enabling the statistical analysis, audience measurements and optimization of the User journey
Processing 3	All the operation enabling the customization of the User journey and of the commercial offers presented

Processing no.1: All the operations which enable the Services to be managed technically and operationally

Description of the Processing

To enable the subscription management and their identification to a User, the Services associate 3 (three) types of identifiers for each user:

- a device identifier (device id): this identifier is device specific
- an “anonymous” identifier: this identifier enables the management of anonymous subscriptions (without a user account), set by the mobile applications store guidelines
- an “external” identifier (user vendor id): such identifier is attributed by the Client to the User.

In addition to these 3 identifiers, the “received” store receipts generated by the mobile app stores following a transaction are related to the Users.

The platform processes every transaction received from the mobile app stores and generates the subscribers’ life cycle and the associated revenue information.

All this data is stored in the Service’s database.

The device identifier is generated at random by the platform upon the first initialization of the Services in the Application.

The “anonymous” identifier is generated at random by the platform SDK during the User’s first registration on the Solution. This identifier is specific to a User, on a device, application, and, accordingly, it is not possible to track a same user, who has not subscribed or is not identified on 2 different applications or 2 different devices.

The “external” identifier is a User account identifier, managed by the Client. It enables the same user to be identified on different platforms, applications, devices.

Purpose of the Processing

Management of the Subscribers’ life cycle and Processing of transactions on the applicative mobile stores

Provision of a support tool for the Client, as a back-up for Users encountering difficulties in accessing their subscription(s) or purchase(s)

Lawfulness for the Processing for the Client

Processing is necessary for the performance of a contract to which the User is a party or in order to take steps at the request of the User prior to entering into a contract with the Client.

Personal Data processed

- Device identifiers
- Anonymous identifier
- External identifier
- Receipts & Transactions of mobile app stores
- History of the subscriptions and purchases made on the different mobile app stores
- Promotional campaigns or paywalls chosen by the Client ;
- Smartphone manufacturer
- Device model
- Device name
- OS
- OS version
- Language
- App version
- App store country
- Subscription information: Subscription type (store SKU), subscription periodicity, subscription start date, renewal date, end date, subscription status (active / inactive), offer status (paid trial, free trial) and associated dates, invoicing status (in billing retry, in grace period), revenue generated, currency.
- Events of the subscribers' life cycle (subscription, renewal, subscription migration, payment issues upon the renewal of a subscription, cancellation of the automatic renewal of subscriptions, termination)

Data subject categories

- The Users

Recipients of the Personal Data processed

- Client (Processing Controller)
- The Supplier (Sub-contractor)
- Amazon Web Services (Subsequent Sub-contractor)
- ClickHouse (Subsequent Sub-contractor)

- Datadog (Subsequent Sub-contractor)
- Sentry (Subsequent Sub-contractor)

Sub-contractors

- **Amazon Web Services, EUROPE region**
  Amazon Web Services EMEA SARL, French subsidiary
  31 Place des Corolles, Tour Carpe Diem, 92400 Courbevoie (France)
  Contact: https://aws.amazon.com/fr/contact-us/
  Tel.: +33 1 46 17 10 00

- **Datadog**
  21 Rue de Châteaudun 6th Floor, 75009 Paris (France)
  Tel.: +1 866 329 44 66

- **Sentry Software**
  4 Place de la Défense, 92800 Puteaux (France)
  Tel.: +33 1 49 01 97 45

- **ClickHouse**
  650 Castro St., Suite 120 #92426, Mountain View CA 94041 (USA)
  Contact: https://clickhouse.com/company/contact

- **CloudFlare**
  6 Pl. de la Madeleine, 75008 Paris
  Tel.: +33 1 73 01 52 44 /+1 (888) 99 FLARE

Personal Data retention period

- The Personal Data processed are kept in the database, for the entire duration of the Agreement between the Client and the Supplier and kept five more years as intermediate archiving by the Supplier to keep the proof of a right or an obligation.
- By exception, the device identifier and anonymous identifiers are safeguarded in the Application's internal storage space (*local storage*), directly on the device, without any limit on the retention period.
- By exception, the technical log data (Datadog and Sentry) are kept for 30 days

Sensitive Personal Data processing

According to Art. 3.2 of the Data Processing Agreement, where a Processing of Sensitive Personal Data is set up by the Controller through the Services (for example through the promotional campaigns or paywalls chosen), the Controller shall ensure that such Processing complies with Art. 9, paragraph 2 of the GDPR.

No Sensitive Personal Data is processed.

Personal Data transfer outside of the EU

In specific situations (transfer to a third party country not covered by a decision on adequacy by the European Commission, and without the guarantees mentioned in Articles 46 and 47 of the GDPR), specific guarantees must be provided and documented in the register (Article 49 of the GDPR)

The Supplier, as the Data Controller's Sub-contractor, shall not transfer Personal Data outside of the EU.

Security measures

The Supplier setup high security measures in order to protect the Users' Personal Data. All these measures are available upon request in Purchasely's ISSMP.

Processing no. 2: All the operations enabling the statistical analysis, audience measurements and optimization of the User journey

Description of the Processing

The Services collect different Personal Data to enable the Client to make statistical analysis, audience measurements and optimize the user journey in its Application.

The data is collected in the form of "front-end" events:

https://docs.purchasely.com/analytics/events/sdk-events/front-end-events

The events are processed to compute the following indicators:

- The global number of sessions per day / month
- The global number of users per day / month
- The global rate of users exposed to a paywall
- The global rate of session exposed to a paywall
- The conversion rate of a paywall
- The average number of sessions before a transaction or a subscription
- The average time before a transaction or a subscription
- The number of sessions of each user
- The number of unique viewers for each paywall created by the Client ;
- The conversion rate for each paywall created by the Client
- The types of User interactions for each paywall created by the Client
- The types of offers and associated conversion rates purchased by the Users on the paywalls created by the Client

Each event is carrying either the User external identifier or the anonymous identifier.

The collection of these front-end events is automatically done by the Services but can be disabled by the Client (globally or per User)

Purposes of the Processing

- Purpose 1: Statistical analysis, audience measurements and optimization of the user journey
- Purpose 2: Services technical operations

Lawfulness for the Processing for the Client

Customer's choice :

Processing is necessary for the purposes of the legitimate interests pursued by the Client, except where such interests are overridden by the interests or fundamental rights and freedoms of the Users which require protection of personal data, in particular where the data subject is a child. Here, the interests or fundamental rights and freedoms of the Users are not threatened because the Client can set up an opt-out.

OR

The User has given consent to the Processing of his or her Personal Data for this specific purposes

Personal Data processed

Each front-end event carries technical data collected by the SDK. Ex:

- Device manufacturer
- Device model
- OS
- OS version
- Language
- App store
- App store country

Data subject categories

- The Users

Recipients of the Personal Data processed

- Client (Processing Controller)
- Supplier (Sub-contractor)
- ClickHouse (Subsequent sub-contractor)
- Amazon Web Services (Subsequent Sub-contractor)
- Datadog (Subsequent Sub-contractor)
- Sentry (Subsequent Sub-contractor)

Sub-contractors

- **Amazon Web Services, EUROPE region**
  Amazon Web Services EMEA SARL, French subsidiary
  31 Place des Corolles, Tour Carpe Diem, 92400 Courbevoie
  Contact: https://aws.amazon.com/fr/contact-us/
  Tel.: +33 1 46 17 10 00

- **Datadog**
  21 Rue de Châteaudun 6th Floor
  Paris, 75009 France
  Tel.: +1 866 329 44 66

- **ClickHouse**
  650 Castro St., Suite 120 #92426, Mountain View CA 94041 (USA)
  Contact: https://clickhouse.com/company/contact

- **CloudFlare**
  6 Pl. de la Madeleine, 75008 Paris
  Tel.: +33 1 73 01 52 44 /+1 (888) 99 FLARE

Personal Data retention period

- The Personal Data is kept for the entire duration of the Agreement between the Client and the Supplier and kept five more year as intermediate archiving by the Supplier to keep the proof of a right or an obligation;
- As the Data Controller's Sub-contractor, the Supplier may proceed at any time with the deletion thereof upon the Client's request
- The technical log data (Datadog and Sentry) is kept for 30 days

Sensitive Personal Data processing

According to Art. 3.2 of the Data Processing Agreement, where a Processing of Sensitive Personal Data is set up by the Controller through the Services (for example through the promotional campaigns or paywalls chosen), the Controller shall ensure that such Processing complies with Art. 9, paragraph 2 of the GDPR.

Personal Data transfer outside of the EU

The Personal Data collected in the context of the Processing no. 2 is systematically anonymized.

Security Measures

The Supplier setup high security measures in order to protect the Users' Personal Data. All of these measures are available upon request in Purchasely's ISSMP.

Processing no. 3: All the operation enabling the customization of the User journey and of the commercial offers presented

Description of the Processing

The Services enable the Client to optimize the performance of its business model, by proposing different promotional campaigns or paywalls to its Users. The Processing no. 3 concerns personal information enabling targeted marketing communications to be presented to the User, directly through the Application.

The User's Personal Data is necessarily transferred by the Client (through the Application) to the Sub-contractor (Supplier) and is not automatically collected (besides the token for the push notification) by the Services. In other words, if no Personal Data is transferred by the Client to the Sub-contractor through the SDK API, no additional data is collected by the Services.

Properties associated by the Client to Users can be wiped via a dedicated SDK API.

Purpose of the Processing

Optimization of the general economic performance of the Client's business model and an increase of the product sales and digital subscriptions.

Lawfulness for the Processing for the Client

Processing is necessary for the performance of a contract to which the User is party or in order to take steps at the request of the User prior to entering into a contract with the Client Performance of the agreement/legitimate interest

Personal Data processed

- Device identifier
- Anonymous identifier
- External identifier
- Receipts & Transactions of mobile app stores

- History of the subscriptions and purchases made on the different mobile app stores
- Smartphone manufacturer
- Device model
- Device name
- OS
- OS version
- Language
- App version
- App store country
- Promotional campaigns or paywalls chosen by the Client ;

Clients can associate properties to their Users, via a dedicated SDK API, in the form of {key, value}.

Ex:

- "gender": "male"
- "intent": "run_marathon"
- "weight: 80kg"
- "eyes_color": "blue"
- "country": "FR"
- "city": "Paris"

Each property is associated with either the User external identifier or the anonymous identifier.

Data Subject categories

- The Users

Recipients of the Personal Data processed

- Supplier (Sub-contractor)
- Amazon Web Services (Subsequent sub-contractor)
- ClickHouse (Subsequent sub-contractor)
- Datadog (Subsequent Sub-contractor)
- Sentry (Subsequent Sub-contractor)

Sub-contractor

- **Amazon Web Services, EUROPE region**
  Amazon Web Services EMEA SARL, French subsidiary
  31 Place des Corolles, Tour Carpe Diem, 92400 Courbevoie
  Contact: https://aws.amazon.com/fr/contact-us/

Tel.: +33 1 46 17 10 00

- **Datadog**
  21 Rue de Châteaudun 6th Floor
  75009, Paris (France)
  Tel.: +1 866 329 44 66

- **Sentry Software**
  4 Place de la Défense, 92800 Puteaux
  Tel.: +33 1 49 01 97 45

- **ClickHouse**
  650 Castro St., Suite 120 #92426, Mountain View CA 94041 (USA)
  Contact: https://clickhouse.com/company/contact

- **CloudFlare**
  6 Pl. de la Madeleine, 75008 Paris
  Tel.: +33 1 73 01 52 44 /+1 (888) 99 FLARE

Personal Data retention period

- By default, the Personal Data are kept three years after the last connexion of the User to the Application
- Client can set up a different Personal Data retention period ; The technical log data (Datadog and Sentry) is kept for 30 days

Sensitive personal data processing

According to Art. 3.2 of the Data Processing Agreement, where a Processing of Sensitive Personal Data is setup by the Controller through the Services (for example If Client associates properties to their Users which can be considered as Sensitive Personal Data), the Controller shall ensure that such Processing complies with Art. 9, paragraph 2 of the GDPR.

Transfer of the Personal Data outside of the EU

The Supplier, as the Data Controller's Sub-contractor shall not transfer Personal Data outside of the EU.

Security measures

The Supplier setup high level security measures in order to protect the Users' Personal Data. All of these measures are available upon request in Purchasely's ISSMP.