PURCHASELY'S DATA PROCESSING AGREEMENT

Updated : May 27th 2025, version 8

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.

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 the Data Processor. 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 (Processor). 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 Processor, 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 are strictly mandatory to allow the Services to be managed technically and operationally
Processing 2	All the operations enabling the statistical analysis, audience measurement and optimization of the User Journey
Processing 3	All the operations enabling the customization of the User journey and of the commercial offers presented
Processing 4	All the operations enabling the recommendation of commercial offers displayed spontaneously

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 (Processor)
- Amazon Web Services (Subsequent Processor)
- ClickHouse (Subsequent Processor)

- Datadog (Subsequent Processor)
- Sentry (Subsequent Processor)

Processors

Entity Name	Services Provided	Location of Processing	Legal Address of the entity processing the data
Amazon Web Services, Inc.	Third-party hosting provider.	United States European Union	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
Cloudflare, Inc.	Content delivery network used for the routing of encrypted API calls to servers, and to optimize content delivery.	Global (www.cloudflare.com/network/)	Cloudflare, Inc. 101 Townsend St San Francisco, CA 94107
DataDog, Inc.	Application performance monitoring, infrastructure and network monitoring, and error capturing. End User metadata may be provided, such as user identifiers, to DataDog for support and application troubleshooting and to improve performance of the Services.	United States European Union	Datadog 21 Rue de Châteaudun 6th Floor 75009 Paris (France) Tel.: +1 866 329 44 66
Functional Software, Inc. (dba Sentry)	Error tracking platform used to capture errors that occur in the Services. End User metadata may be provided such as user identifiers to Sentry for support and application troubleshooting and improving performance.	United States European Union	Sentry Software 4 Place de la Défense 92800 Puteaux (France) Tel.: +33 1 49 01 97 45
ClickHouse	High-performance and real-time data warehouse	European Union	Herengracht 576, 1017 CJ Amsterdam (Netherlands) Contact: https://clickhouse.com/company/contact

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 Processor, 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)

The Suppliers relies on a globally distributed Content Delivery Network (CDN), to optimize response times by executing processing as close to end users as possible. For users located outside of the EU, processing may occur locally in their region to improve

performance. However, no personal data is transferred from the EU to third countries, as the data originates from the user's location outside the EU. Additionally, no data is stored outside the EU, and processing remains transient and stateless. This setup ensures compliance with our obligation to avoid international transfers of EU data.

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

Client'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 (Processor)

- ClickHouse (Subsequent Processor)
- Amazon Web Services (Subsequent Processor)
- Datadog (Subsequent Processor)
- Sentry (Subsequent Processor)

Processors

Entity Name	Services Provided	Location of Processing	Legal Address of the entity processing the data
Amazon Web Services, Inc.	Third-party hosting provider.	United States European Union	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
Cloudflare, Inc.	Content delivery network used for the routing of encrypted API calls to servers, and to optimize content delivery.	Global (www.cloudflare.com/network/)	Cloudflare, Inc. 101 Townsend St San Francisco, CA 94107
DataDog, Inc.	Application performance monitoring, infrastructure and network monitoring, and error capturing. End User metadata may be provided, such as user identifiers, to DataDog for support and application troubleshooting and to improve performance of the Services.	United States European Union	Datadog 21 Rue de Châteaudun 6th Floor 75009 Paris (France) Tel.: +1 866 329 44 66
Functional Software, Inc. (dba Sentry)	Error tracking platform used to capture errors that occur in the Services. End User metadata may be provided such as user identifiers to Sentry for support and application troubleshooting and improving performance.	United States European Union	Sentry Software 4 Place de la Défense 92800 Puteaux (France) Tel.: +33 1 49 01 97 45
ClickHouse	High-performance and real-time data warehouse	European Union	Herengracht 576, 1017 CJ Amsterdam (Netherlands) Contact: https://clickhouse.com/company/contact

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 Processor, 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 Suppliers relies on a globally distributed Content Delivery Network (CDN), to optimize response times by executing processing as close to end users as possible. For users located outside of the EU, processing may occur locally in their region to improve performance. However, no personal data is transferred from the EU to third countries, as the data originates from the user's location outside the EU. Additionally, no data is stored outside the EU, and processing remains transient and stateless. This setup ensures compliance with our obligation to avoid international transfers of EU data.

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 Processor (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 Processor 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.

The Supplier relies on a globally distributed Content Delivery Network (CDN), to optimize response times by executing processing as close to end users as possible. For users located outside of the EU, processing may occur locally in their region to improve performance. However, no personal data is transferred from the EU to third countries, as the data originates from the user's location outside the EU. Additionally, no data is stored outside the EU, and processing remains transient and stateless. This setup ensures compliance with our obligation to avoid international transfers of EU data.

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

Client'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

- 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 (Processor)
- Amazon Web Services (Subsequent Processor)
- ClickHouse (Subsequent Processor)
- Datadog (Subsequent Processor)
- Sentry (Subsequent Processor)

Processors

Entity Name	Services Provided	Location of Processing	Legal Address of the entity processing the data
Amazon Web Services, Inc.	Third-party hosting provider.	United States European Union	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
Cloudflare, Inc.	Content delivery network used for the routing of encrypted API calls to servers, and to optimize content delivery.	Global (www.cloudflare.com/network/)	Cloudflare, Inc. 101 Townsend St San Francisco, CA 94107
DataDog, Inc.	Application performance monitoring, infrastructure and network monitoring, and error capturing. End User metadata may be provided, such as user identifiers, to DataDog for support and application troubleshooting and to improve performance of the Services.	United States European Union	Datadog 21 Rue de Châteaudun 6th Floor 75009 Paris (France) Tel.: +1 866 329 44 66
Functional Software, Inc. (dba Sentry)	Error tracking platform used to capture errors that occur in the Services. End User metadata may be provided such as user identifiers to Sentry for support and application troubleshooting and improving performance.	United States European Union	Sentry Software 4 Place de la Défense 92800 Puteaux (France) Tel.: +33 1 49 01 97 45
ClickHouse	High-performance and real-time data warehouse	European Union	Herengracht 576, 1017 CJ Amsterdam (Netherlands) Contact:

			https://clickhouse.com/company/contact

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 Suppliers relies on Cloudflare Workers, a globally distributed Content Delivery Network (CDN), to optimize response times by executing processing as close to end users as possible. For users located outside of the EU, processing may occur locally in their region to improve performance. However, no personal data is transferred from the EU to third countries, as the data originates from the user's location outside the EU. Additionally, no data is stored outside the EU, and processing remains transient and stateless. This setup ensures compliance with our obligation to avoid international transfers of EU data.

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.

Processing no. 4: All the operation enabling the proactive recommendation of commercial campaigns

Description of the Processing

The Service enables the Clients the ability to schedule, and deliver pro-active in-app marketing campaigns and experiments targeted to specific User segments and triggered by specific events. This feature involves the processing of User interaction data and targeting parameters defined by the Client in order to deliver the campaign content through the Client's app interface.

Purpose of the Processing

The purpose of the processing is to enable Clients to personalize User experience and optimize engagement and monetization through A/B tests, promotions, and other campaign types, leveraging Purchasely's orchestration and targeting engine.

Lawfulness for the Processing for the Client

Client'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

- Anonymous identifier
- External identifier
- Smartphone manufacturer
- Promotional campaigns viewed by the user (campaign identifier, campaign first display date, campaign last display date, number of times a campaign has been displayed)

Data subject categories

- The Users

Recipients of the Personal Data processed

- Client (Processing Controller)
- The Supplier (Processor)
- Amazon Web Services (Subsequent Processor)
- Datadog (Subsequent Processor)
- Sentry (Subsequent Processor)
- ClickHouse (Subsequent Processor)

Processors

Entity Name	Services Provided	Location of Processing	Legal Address of the entity processing the data
Amazon Web Services, Inc.	Third-party hosting provider.	United States European Union	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
Cloudflare, Inc.	Content delivery network used for the routing of encrypted API calls to servers, and to optimize content delivery.	Global (www.cloudflare.com/network/)	Cloudflare, Inc. 101 Townsend St San Francisco, CA 94107
DataDog, Inc.	Application performance monitoring, infrastructure and network monitoring, and error capturing. End User metadata may be provided, such as user identifiers, to DataDog for support and application troubleshooting and to improve performance of the Services.	United States European Union	Datadog 21 Rue de Châteaudun 6th Floor 75009 Paris (France) Tel.: +1 866 329 44 66
Functional Software, Inc. (dba Sentry)	Error tracking platform used to capture errors that occur in the Services. End User metadata may be provided such as user identifiers to Sentry for support and application troubleshooting and	United States European Union	Sentry Software 4 Place de la Défense 92800 Puteaux (France) Tel.: +33 1 49 01 97 45

	improving performance.		
ClickHouse	High-performance and real-time data warehouse	European Union	Herengracht 576, 1017 CJ Amsterdam (Netherlands) Contact: https://clickhouse.com/company/contact

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.
- 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

The Processor relies on a globally distributed Content Delivery Network (CDN), to optimize response times by executing processing as close to end users as possible. For users located outside of the EU, processing may occur locally in their region to improve performance. However, no personal data is transferred from the EU to third countries, as the data originates from the user's location outside the EU. Additionally, no data is stored outside the EU, and processing remains transient and stateless. This setup ensures compliance with the Processor obligation to avoid international transfers of EU data.

Security measures

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