Eskimi DMP & Data Legality, Validity & Security - Technical

DMP

Eskimi DMP

Eskimi Data Management Platform is an in-house DMP which doesn't use any third party technologies. Eskimi DMP is used by only Eskimi DSP to foster personalized advertising for Eskimi advertisers. Eskimi works with industry leading partners, such as Doubleclick, Magnite, OpenX and others. Eskimi DMP is bounced to the data that is provided by the partners that Eskimi DSP is connected to.

Eskimi DMP Data

Eskimi DMP collects, agregates the data in real-time. In-house algorithms not only crunches the data in real-time, but follows the necessary privacy regulations such as GDPR, CCPA. Eskimi DMP collects, agregates, stores the below data signals:

Technical name	Explanation	Technical example
dmpId	User identifier. Mobile advertising ID on apps, cookie ID on web	`"dmpId":"4726ce65-ae90-4536-8d8c-6e5b204cca83"`
countries	list of countries DmpID was seen in	`"countries":{"ng":303396,"--":55}`
countrySeenTime	Last seen time DmpID was seen in country	`"countrySeenTime":{"ng":18659,"--":18628}`

cities	List of cities DmpID was seen in, based on GPS data	`"cities":{"ng.ozomu":20596}`
citySeenTime	Last seen time DmpID was seen in a city	`"citySeenTime":{"ng.ozomu":18656}`
tmpCities	list of cities DmpID was seen in, based on all other data (IP, user input, etc)	`"tmpCities":{"ng.lagos":148468,"ng.":473,"ng.awka":2258` }
tmpCitySeenTime	Last seen time DmpID was seen in TmpCity	`tmpCities":{"ng.lagos":148468,"ng.":473}`
yobs	Years of birth. Can be multiple depending on user input	`"yobs":{"1959":52524,"0":21}`
genders	Genders. Can be multiple depending on user input	`"genders":{"1":50731,"0":57}`
pageViews	Total number of page views	`"pageViews":303600`
operatorPageViews	Shows how many page views per day each operator ID has	`operatorPageViews":{"365":{"18610":335,"18629":44` }
operatorIds	Telco operator IDs	`operatorIds":{"365":87514,"0":3005`

operatorSeenTime	Last seen time for operator	`"operatorSeenTime":{"365":18659,"0":18628}`
operatorFirstSeenTime	First seen time for operator	`"operatorFirstSeenTime":{"365":18659}`
modelIds	Device model	`"modelIds":{"20101":299968}`
modelSeenTime	Last time device model was seen with DmpID	`"modelSeenTime":{"20101":18659}`
operatorModelIds	what device was used with specific operator	`"operatorModelIds":{"365.20101":81961,"357.20101":16819}`
operatorModelSeenTime	When was the last time device was seen	`"operatorModelSeenTime":{"365.20101":18659"}`
keywords	Verticals or interest categories, e.g. https://storage.googleapis.com/adx-rtb-dictionaries/publisher-verticals.txt	`"keywords":{"1164":16,"930":12}`
keywordSeenTime	last seen time for keyword	`"keywordSeenTime":{"1164":18656,"930":18649}`

connectionTypes	How users connected to internet. 2G, 3G, 4G, wifi, etc	`"connectionTypes":{"2":72903,"3":10358}`
connectionTypeSeenTime	last seen time per connection type	`"connectionTypeSeenTime":{"2":18659,"3":18659}`
deviceId	Legacy. Original Device ID of the user. matches DmpID.	`"deviceId":"4726ce65-ae90-4536-8d8c-6e5b204cca83"`
siteIds	Internal site ID where user was browsing. Might be converted to exact app bundle or site domain	`"siteIds":{"52299180":41,"34189419":2427}`
siteSeenTime	When was the last time user visited a specific site.	`"siteSeenTime":{"52299180":18659,"34189419":18632`
firstSeen	First time DmpID was seen	`"firstSeen":18073`
lastSeen	last time DmpID was seen	`"lastSeen":18659`
lastAvg	number of page views per day	`"lastAvg":569`

The data in the table is used for clear purpose:

- Analytical tools, such as Telcodash.
- Targeting, that are needed to executed personalized advertising.

Eskimi DMP Collection Schema

Eskimi DMP collect the data in real-time. The following flow is:

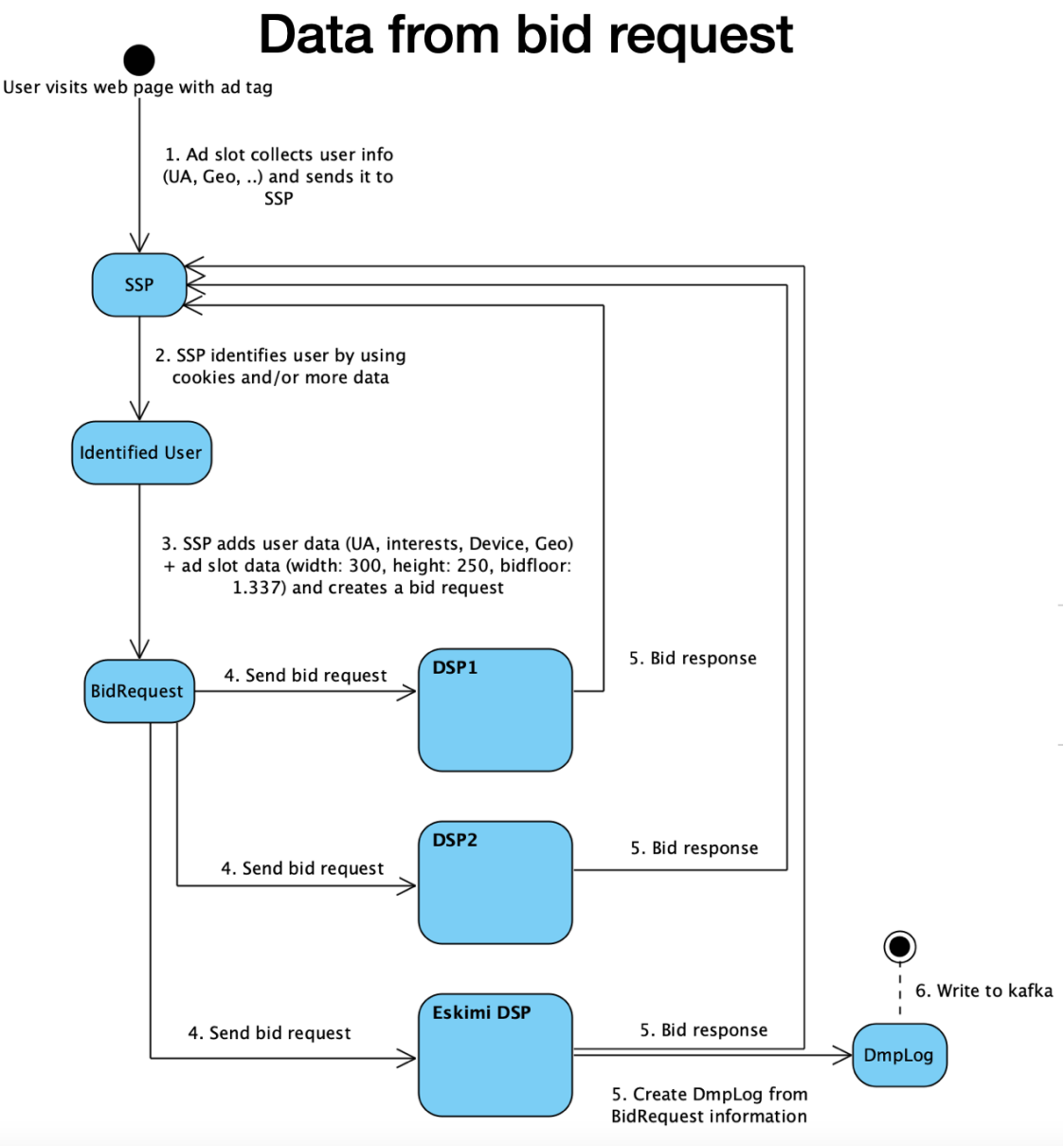
1. A user visits a website page that has an implemented SSP JavaScript tag OR visits an app that has an implemented SSP SDK. These JS tags and SDKs has ad slots that collects user information which includes, but it is not limited to User agent, geo location, IP and etc.

2. JS/SDK sends the information to the SSP. SSP identifies the user by using cookies and/or more data (ex.: Mobile Advertising ID).

3. SSP adds users data (UA, interests and etc.) with the ad slot data (width: 300, height: 250, bidfloor 1.337). This information is transfered to the SSP.

4. The ad signal is sent to different DSPs that compete for the ad signal in an openRTB auction that happens in miliseconds everytime the browser is loaded/refreshed. The goal of any DSP is to win the auction and serve their advertiser ad.

5. Eskimi DSP sends data from the ad signal to Eskimi DMP. Where DMP profiles are created, if the user is seen for the first time. If the user was seen in the past the data will be added to the historical data that Eskimi DMP has collected.



Legal, Valid & Secure Data

Aktyvus sektorius UAB, doing business as Eskimi, as a global provider of digital advertising media and data management technology. In our activities, Eskimi is committed to protecting the privacy of individuals and their personal information. While, ensuring any personal information is safe and used strictly in accordance with the applicable laws, such as GDPR, CCPA, and other applicable guidelines.

1. How you can justify that your data is legal?

Eskimi strictly adhere to the relevant EU users' consent regulations and policies (GDPR) and is a member of TCF (Transparency & Consent Framework). TCF membership ensures that Eskimi comply with the EU’s GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user’s device, such as cookies, advertising identifiers, device identifiers, and other tracking technologies.

Full TCF vendor list: https://iabeurope.eu/vendor-list-tcf-v2-0/ Search for *UAB Aktyvus Sektorius.*

More about TCF: https://iabeurope.eu/transparency-consent-framework/

More about Eskimi Privacy Policy: https://www.eskimi.com/privacy-policy

2. How can you justify that your data is valid?

The types of pseudonymous personal information used via the Platform are cookie IDs, Mobile Advertising Identifiers, and IPs.

Cookie is a browser storage mechanism that allows Eskimi to store a pseudonymous identifier to identify the user. The cookie identifier is not directly linkable to any particular individual

Mobile Advertising Identifier (MAID, commonly known as Device ID) is a pseudonymous, user-resettable identifier for online advertising purposes. The identifier is created by the operating system (iOS or Android) and can be retrieved by installed apps.

IP address is a very approximate location of the technical device, used to communicate where internet requests and responses are coming from and where should they go to next.

Eskimi receives the above described personal data from clients (advertisers and publishers), partners (publisher ad exchanges, such as google, or agencies/advertiser groups). All involved party partnerships are covered contractually. Every partner Eskimi works with ensures the legality of the data that is sent to Eskimi - including ways in which data is gathered and processed. Examples of processes are:

* Transaction validation. Every impression that comes between Eskimi and publisher platforms or publisher partners is technically validated with a follow-up call to the partner
* Regular audits. Data structures and legality of the data is regularly audited by the biggest Eskimi partners
* Internal TOMs (please see below)

3. What is the purpose of data collection?

The data is collected and used for clear purpose for which the user agrees upon.

We use the data only when the user consented to the below sections:
1: identification
3: create personalised ads profile
4: Select personalised ads

While when the user gives legitimate interest the purpose of data usage becomes more flexible. With it Eskimi can:
2: Select basic ads
7: measure ad performance
10: develop and improve products

4. How can you justify that your data is secure?

Here are the TOMs in place to make sure the data is secure:

Technical and Organizational Measures for Data Security

Pursuant to the provisions of Eskimi Privacy Policy, GDPR and other applicable data protection laws Eskimi shall implement the following measures to secure the processed data. The following list constitutes the minimal level of security measures. Additional measures may be applied for the specific categories of the data.

Physical access control

- Physical protection of the company premises (e.g., lockable door)
- Additional protection of the premises (e.g., alarm system, gate
- keeper, security guard)
- Access authorization structure (incl. server access)

Storage control

- Pseudonymization of personal data

Access control

- Authentication of users (e.g., username & password)
- Password policy or system side requirement of password
- requirements
- Password complexity (at least 3 of the 4 criteria: Upper case letter, lower case letter, special
- character, and number)
- Password with minimum length of 8 characters
- No time-based change of passwords
- Group-wide auto logout after defined time
- Role-based authorization management or regular recertification of authorizations

User control

- All employees are bound to confidentiality or are subject to a duty of confidentiality
- Need to know principle implemented

Transmission control

- Encryption of critical data during data transmission

Recoverability

- Data backup policy incl. regular backups
- Secure storage of data backups

Reliability

- Network Monitoring / Intrusion Detection System (IDS / IPS)
- Change management
- Data protection management system
- Regular updates or patch and vulnerability management

Availability control

- Redundant design of all important systems

Contract control

- Selection of processors according to due diligence aspects

Data integrity

- Antivirus or antimalware protection

Accountability

- Logging of access attempts to IT systems
- Logging of activities on the server
- Logging of processing operations (reading, modification, and deletion of data)

Separability

- Separation into test, production, and development levels
- Separation of data processing (logical or physical), multiclient capability

Further Measures

- Regular testing, assessing & evaluation of effectiveness of technical and organizational measures
- Appropriate processes or policies to ensure data subjects' rights
- Regular training on the user privacy.

Approved by:
Tomas Ivanauskas
Data Protection Officer

Last updated: 23 August 2021

Revision #19
Created 31 August 2021 11:17:31 by Gabriele
Updated 23 September 2022 10:59:42 by Gabriele