Eskimi DMP & Data Legality, Validity & Security - Business

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 information that includes, but it is not limited to, like Mobile Advertising ID, GPS location, IP, city, country, gender & age, device and other data points. These signals are included into the DMP profile which refers to a distict customer. These data signals are used to deliver:

- Better, more effective personalized advertising.
- Analytics such as Telcodash.

Eskimi DMP Collection Schema

Eskimi DMP collect the data in real-time. Below you will find how the data flows:

1. A user visits a publisher - website page (ex.: bbc.com) or an app (ex.: Viber). These apps and sites has ad slots that collects user information which includes, but it is not limited to User agent, geo location, IP and etc.

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

3. SSP adds users data with the ad placement data. From this information SSP creates a ad signal.

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 eligable data from the ad signal Eskimi DMP. Where DMP profiles, 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
2: Select basic ads
3: create personalised ads profile
4: Select personalised 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 #5
Created 16 September 2022 15:22:42 by Gabriele
Updated 2 January 2024 12:07:56 by Vytautas