Privacy and cookies

- Eskimi DMP & Data Legality, Validity & Security - Technical
- 3rd party cookie deprecation
    - Everything you need to know about third-party cookies
    - The end of Third-Party cookies
- iOS 14.5 Changes
    - Apple decides to change the rules
- Eskimi DMP & Data Legality, Validity & Security - Business
- What cookies are used in Eskimi
- Alternative identity providers
    - UID 2.0 integration
- Redmob Data Legality, Validity & Security

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:

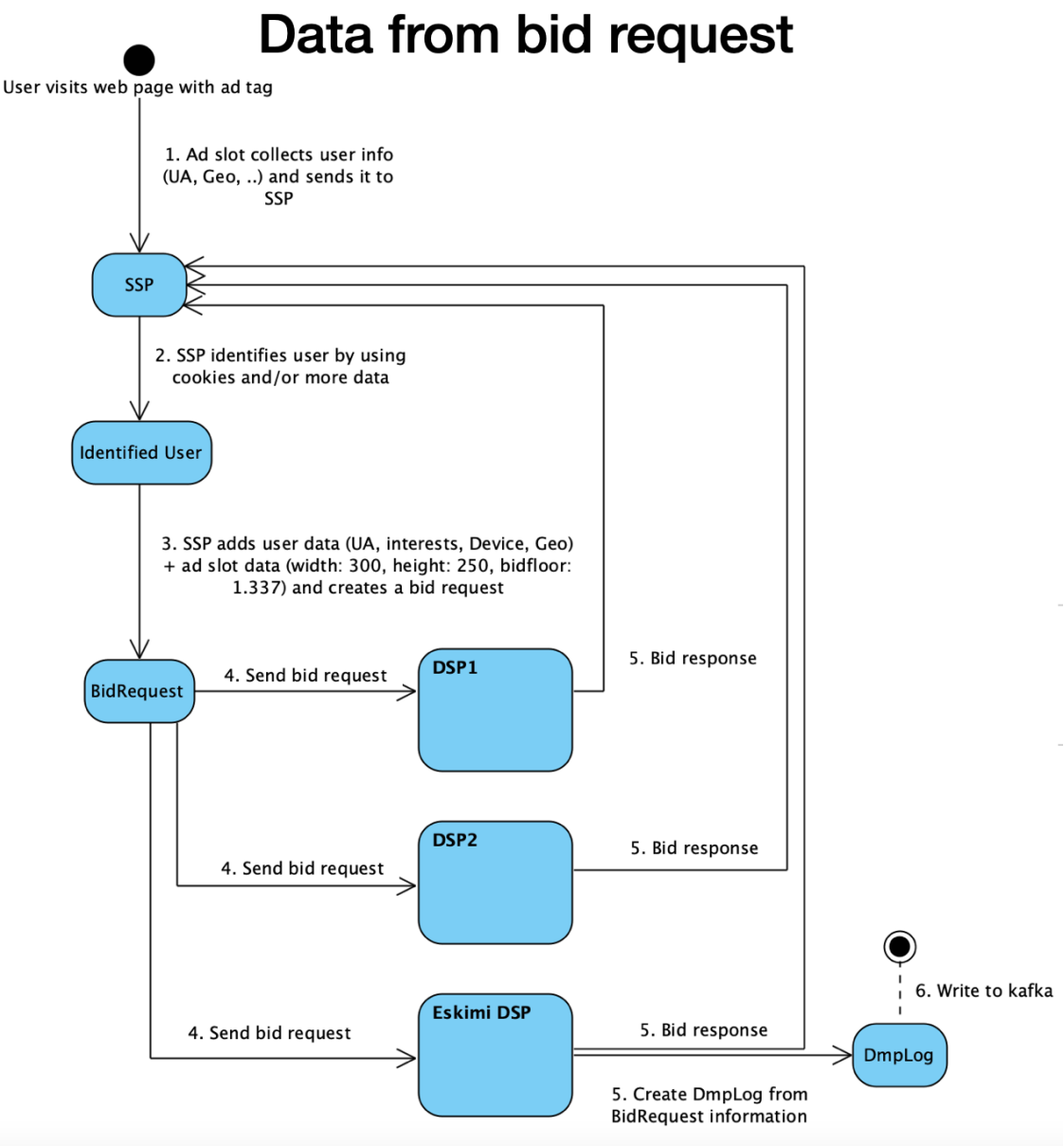
1. A user visits a website page that has an implemented SSP JavaScript tag OR visits an app that has an implemented SSP SDK. These JS tags and SDKs has ad slots that collects user information which includes, but it is not limited to User agent, geo location, IP and etc.

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

3rd party cookie deprecation

Everything you need to know about third-party cookies

What are third-party cookies?

Websites use cookies to remember a user's action so they aren't asked to perform a task again and again. As a result, they help provide a better, more personalized user experience.

Third-party cookies are cookies that are stored under a **different domain than you are currently visiting**. So you might be browsing on `example.com`, but third-party cookies are set by `cookieweb.com`. They are mostly used a) to track users between websites b) display more relevant ads between websites. The most common third-party entities are advertisers, marketers, and social media platforms.

It is essential to remember that **third-party cookies are not the same as first-party cookies**. **First-party cookies**, on the other hand, are stored under the same domain you are currently visiting. So, if you are on `example.com`, all cookies stored under this domain are considered first-party cookies. Those cookies are usually used to: a) identify a user between pages, b) remember selected preferences, c) store your shopping cart. You can hardly find a website nowadays that does not use first-party cookies.

Why are third-party cookies used?

Cross-site tracking: the practice of collecting browsing data from numerous sources (websites) that details your activity.

Retargeting: using search activity to retarget visitors with visual or text ads based on the products and services for which they've shown interest

Ad-serving: making decisions regarding the ads that appear on a website, deciding when to serve these ads, and collecting data (and reporting said data including impressions and clicks) in an effort to educate advertisers on consumer insights and ad performance.

How do third-party cookies work?

Third-party cookies work by embedding JavaScript from one website into another. Third-party cookies store data remembered between browsing sessions. They remember information this way because HTTP, the web browsing protocol, is a stateless protocol. A “stateless protocol” means that data is not saved between browsing sessions. In the HTTP response header, cookie attributes determine whether a cookie is a first- or third-party cookie.

Third-party cookies… one common example. Let’s say earlier in the week you looked up some vacation rentals in South Africa. You browsed a few websites, admired the photos of the sunsets and sandy beaches, but ultimately decided to wait another year before planning your vacation. A few days go by and suddenly it seems like you are seeing ads for South Africa vacations on many of the websites you visit. Is it a mere coincidence? Not really. The reason you are now seeing these ads on vacationing in South Africa is that your web browser stored a third-party cookie and is using this information to send you targeted advertisements.

You’re unintentionally creating a “trail of crumbs.” Most web users don’t realize that a browser window with multiple tabs open constitutes a single “session.” As you move from tab to tab, you are unwittingly relaying information about your web visit history to other websites and parties. And, closing the web browser doesn’t always eliminate the cookies your computer stores following the session. Depending on the browser you use, you may have to activate this manually.

You may be on a website with 3rd party cookies and not even know it. One of the failings of cookie notices is that they don’t often specify what types of cookies are being used on the site. They could be first-party, third-party, or both. But, if the website has advertisements (which many do), then you can reasonably expect the website to be generating both first- and third-party cookies.

Are third-party cookies actually useful?

Since the late 1990s, online marketers have built their businesses on the ability to track online users and then target them with advertisements, and much of this has been through the use of third-party cookies. Let’s play “devil’s advocate” for a moment. Could third-party cookies actually be useful for users? In a way, yes. The two largest online advertising firms, Google Ads and AdSense, make a valid point that 3rd party cookies are useful to consumers as they create advertisements that are in line with individual interests. After all, if you are forced to see the ads, it's better if they are related to your interests.

The end of Third-Party cookies

Pressure from regulators and consumers has led many within the tech industry to declare third-party cookies will soon come to an end. In this section we will discuss the changes that major players are doing and how it will impact digital advertising market.

Why third-party cookies are going away?

3rd Party Cookies power all the ways we track, target, and measure performance in digital advertising. However, they track users silently. As an industry, we didn't do a great job of educating users how and why we use cookies. And we didn't give people a way to opt-out.

As a consumer, you have little control over who is collecting this information or where it is going—you are able to clear cookies from your own browser, but you'll never be able to manage or delete servers holding third-party data that has already been gathered.

In response to the perceived lack of transparency and control for individuals, data breaches, and "creepiness" in advertising, privacy legislation from the EU and California now give users control over their data. Effectively, these policies give users the ability to block various tracking technologies or request the deletion of their data. Tech companies such as Apple and Mozilla have also responded by giving users control of how their data is used both within browsers and devices.

Implementing and increasing security features to protect the privacy of users is nothing new and has been going on for years now, and for the most part **website users will actually benefit from it**. One of the first companies to do so is Apple and Mozilla, while others are yet to follow.

Full third-party cookie blocking by Safari

Apple first launched Safari Intelligent Tracking Prevention (ITP) within Safari on 2017, where it immediately set a new bar for web privacy standards on both desktop and mobile by blocking some, but not all, cookies by default.

With the beginning of spring of 2020 Apple launched a major update to its ITP, the privacy feature that allows the company's web browser to block cookies and prevent advertisers from snooping on your web habits. In simple sense - **Safari by default blocked all third-party cookies**. That

means that no advertiser or website is able to follow you around the internet using the commonplace tracking technology.

To blocking third-party cookies across the board and by default, ITP now has safeguards against trackers using the very nature of tracking prevention as a way to keep tabs on users. The new feature set also ensures that websites and trackers can't use login IDs to digitally fingerprint users who might otherwise be using tracking prevention or other privacy tools.

Firefox blocks third-party cookies

On 2019 Firefox announced that their Enhanced Tracking Protection will automatically be turned on by default for all users worldwide as part of the 'Standard' setting in the Firefox browser and will block known "third-party tracking cookies".

Enhanced Tracking Protection works behind-the-scenes to keep a company from forming a profile of you based on their tracking of your browsing behavior across websites — often without your knowledge or consent. Those profiles and the information they contain may then be sold and used for purposes you never knew or intended. Enhanced Tracking Protection helps to mitigate this threat and puts you back in control of your online experience.

Mozilla follows a different approach when blocking trackers and cookies than Apple does. Instead of blocking or limiting **all third-party** and **client side cookies** by default, Firefox uses the Disconnect list to determine whether a cookie should be blocked or not. This curated list contains thousands of known tracking companies and is updated on a regular basis. The reasoning behind this decision is **to keep the web experience as seamless and functional as possible**, since some cookies are crucial for web building.

Chrome will block third-party cookies

It is not a surprise that with the changes that Apple and Mozilla launched Google would follow. The company revealed its "Privacy Sandbox" in August 2019, an initiative to personalize (or target) web ads while still preserving user privacy. In January 2020, Google announced that it hoped to block third-party cookies from its Chrome browser by 2022 — a move that other browsers, like Safari and Firefox, made years ago. Google has planned to replace third-party cookies with technology developed through Privacy Sandbox.

That's where Google's Federated Learning of Cohorts (FLoC) comes in, which Google says is a "privacy-first" and "interest-based" advertising technology. With FLoC, Chrome will keep track of a user's browsing habits across the web, and then place the user in various audiences, or "cohorts," based on those habits. Advertisers will then target their ads to cohorts, rather than an individual user. So if you're looking for a browser that doesn't collect your data for ads — as an individual or as part of an anonymous audience — you might want to try a different one. (By the way, you can turn off ad personalization, activity tracking, and delete the data Google has collected about you

here.)

In many cases this development is a direct reaction to new security holes, workarounds, aggressive tracking and shady business techniques and will most likely continue in the future.

Finally, while Google says it is committed to developing and using ad tech that doesn’t rely on tracking and advertising to users, other companies are developing their own non-cookie tracking methods that do, and you could still be tracked by them when you use Chrome (or another browser). The core companies will be presented in another chapter.

iOS 14.5 Changes

Apple decides to change the rules

On 2021 Apple released iOS 14.5, its big new software update for iPhones. It adds a lot of new features, but the one that’s been grabbing headlines is its new privacy change, which gives users more transparency and control over apps that want to track them for advertising.

Apple's long-debated, long-awaited App Tracking Transparency feature and policy will now be fully enforced starting with the release of iOS 14.5.

A large portion of the apps in the App Store for these devices utilizes a tracking technique called ID for Advertisers (IDFA) to track users' activity between multiple apps published by multiple companies, to inform ad targeting and other monetization and data collection techniques.

On 2020, Apple announced that it would begin requiring all apps to ask for users' permission in advance to do this on an app-by-app basis. Anticipating that many users would opt out and that the change would therefore significantly impact revenue, various app developers and ad networks have criticized the move, saying it will hurt big and small businesses alike.

Those critics are not making that up: the move is likely to have a significant impact on the bottomline for many types of apps that rely on advertising for revenue. But Apple maintains that users' control over how they are tracked and how their data is used and accessed is the most important concern at hand.

Current Situation

These Apple changes will impact us as well. However, the primary thing what we can do is to give a better view what is happening in the market. The below table gives insights on how many identified bid requests Eskimi has received in 7 day period. Identifier is important when it comes to targeting and capping.

Identified Requests - bid requests that had IDFA and received in 7 day period.

Total Requests - all bid requests received in 7 day period.

Identity Rate - indicates percentage of identified traffic from all received traffic. Calculated: IDENTIFIED REQUESTS / TOTAL REQUESTS * 100%

COUNTRY	IDENTIFIED REQUESTS	TOTAL REQUESTS	IDENTITY RATE (%)
Argentina	44,610,612	80,865,006	**55.17**
Armenia	97,994,608	143,848,684	**68.12**
Australia	575,038,935	1,162,533,109	49.46
Azerbaijan	24,909,631	38,157,544	**65.28**
Bahrain	41,786,451	70,406,424	**59.35**
Bangladesh	47,613,371	74,610,133	**63.82**
Belarus	33,679,367	59,103,149	**56.98**
Brazil	57,215,499	93,430,096	**61.24**
Bulgaria	3,317,651	5,271,467	**62.94**
Burkina Faso	210,423	273,501	**76.94**
Cambodia	85,384,004	119,311,183	**71.56**
Cameroon	26,399,547	37,336,257	**70.71**
Chad	1,057,992	1,550,040	**68.26**
Chile	31,786,699	48,146,759	**66.02**
Colombia	23,817,273	39,794,663	**59.85**
Czechia	7,628,307	17,717,246	43.06
Democratic Republic of the Congo	15,947,395	22,144,410	**72.02**
Egypt	88,642,398	166,917,357	**53.11**
Gabon	5,856,980	9,276,305	**63.14**
Georgia	116,062,689	190,395,292	**60.96**
Ghana	227,602,588	334,230,122	**68.1**

Greece	16,064,618	18,947,714	**84.78**
Hungary	1,638,124	3,652,653	44.85
India	186,079,630	295,290,523	**63.02**
Indonesia	249,724,395	365,905,857	**68.25**
Ivory Coast	24,245,771	33,129,942	**73.18**
Jordan	5,034,178	5,334,573	**94.37**
Kazakhstan	42,537,013	69,104,383	**61.55**
Kenya	39,921,477	75,633,024	**52.78**
Kuwait	99,995,277	136,297,360	**73.37**
Kyrgyzstan	15,685,647	24,784,200	**63.29**
Lithuania	34,648,500	74,985,228	46.21
Malaysia	236,523,119	385,159,845	**61.41**
Myanmar	30,858,210	47,328,172	**65.2**
Nepal	30,299,603	49,106,385	**61.7**
Nigeria	312,966,031	471,824,897	**66.33**
Oman	8,249,217	15,487,769	**53.26**
Pakistan	25,109,488	40,552,414	**61.92**
Philippines	185,888,690	315,910,139	**58.84**
Poland	55,745,563	78,558,049	**70.96**
Qatar	75,411,112	132,076,932	**57.1**
Republic of the Congo	5,371,765	7,709,673	**69.68**
Romania	4,027,420	9,728,136	41.4
Russian Federation	89,191,122	102,556,054	**86.97**

Saudi Arabia	315,063,355	438,320,650	**71.88**
Singapore	190,963,974	374,667,330	**50.97**
Slovakia	2,382,415	5,152,441	46.24
Slovenia	6,509,927	8,359,918	**77.87**
South Africa	408,149,408	933,822,925	43.71
Sri Lanka	38,227,617	54,972,291	**69.54**
Sweden	39,054,833	54,977,267	**71.04**
Taiwan	2,768,812	4,884,174	**56.69**
Thailand	388,533,368	694,701,492	**55.93**
Turkey	193,218,578	334,749,962	**57.72**
Uganda	29,241,552	40,892,176	**71.51**
Ukraine	392,582,624	683,211,344	**57.46**
United Arab Emirates	166,992,511	302,587,749	**55.19**
Venezuela	2,201,641	2,294,660	**95.95**
Vietnam	285,021,407	442,718,700	**64.38**
Zambia	14,097,318	21,751,328	**64.81**

Full country list: https://docs.google.com/spreadsheets/d/1jEJrXikDWvqie4oy846fjxtktqq6d02iQxL-JJ8Ak2o/edit?usp=sharing

DATE	IDENTIFIED REQUESTS	TOTAL REQUESTS	IDENTITY RATE (%)
2021-06-14	1,584,739,674	2,760,978,769	57.4
2021-06-15	1,552,134,889	2,639,048,788	58.81
2021-06-16	1,874,397,040	3,141,122,722	59.67
2021-06-17	1,848,458,712	3,126,053,446	59.13
2021-06-18	1,924,325,671	3,193,631,646	60.26
2021-06-19	1,992,838,848	3,292,191,770	60.53

2021-06-20	1,949,012,331	3,315,953,177	58.78

Insights

88% of all the countries had >50% identified traffic. This indicates that in 88% of all markets over 50% of all received traffic had an identifier.

63% of all the countries had >60% identified traffic. This indicates that in 63% of all markets over 60% of all received traffic had an identifier.

25% of all the countries had >70% identified traffic. This indicates that in 25% of all markets over 70% of all received traffic had an identifier.

6% of all the countries had >80% identified traffic. This indicates that in 6% of all markets over 80% of all received traffic had an identifier.

While when it comes to daily analytics there is no significant drop for the identified rate. The average identity rate seeks 58%-60% on a global scale.

The key insight that can be draw from the results is - **users are hesitating to adopt iOS 14.5**. This is why the rate is still high in all of the markets.

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

What cookies are used in Eskimi

Cookie category	Cookie name	Cookie purpose	Cookie expiry
Functional	#.#-#-#-#-#.ack	Used to contain user’s survey and quiz answers in Local Storage.	Persistent
	#.#-#-#-#-#.inProgress	Used to contain user’s survey and quiz answers in Local Storage.	Persistent
	#.#-#-#-#-#.queue	Used to contain user’s survey and quiz answers in Local Storage.	Persistent
	#.#-#-#-#-#.reclaimEnd	Used to contain user’s survey and quiz answers in Local Storage.	Persistent
	#.#-#-#-#-#.reclaimStart	Used to contain user’s survey and quiz answers in Local Storage.	Persistent
	__cf_bm	This cookie is used to distinguish between humans and bots. This is beneficial for the website, in order to make valid reports on the use of their website.	1 day
	__eConsent	Stores the user's cookie consent state for the current domain	29 days
	CONSENT [x2]	Used to detect if the visitor has accepted the marketing category in the cookie banner. This cookie is necessary for GDPR-compliance of the website.	2 years
	bscookie	This cookie is used to identify the visitor through an application. This allow s the visitor to login to a website through their LinkedIn application for example.	1 year

CookieConsent [x2]	Stores the user's cookie consent state for the current domain	1 year
debug	This cookie is used to detect errors on the website - this information is sent to the website's support staff in order to optimize the visitor's experience on the website.	Persistent
li_gc	Stores the user's cookie consent state for the current domain	179 days
test_cookie	Used to check if the user's browser supports cookies.	1 day
__eDId	cookie ID	30 days
__eP	cookie matching lock cookie	14 days
__eConsent	EU GDPR TCF consent string cookie	30 days
eucid_*	click ID cookies	30 days
dnt	do not track (opt-out) cookie	365 days

Alternative identity providers

this chapter describes which identity providers Eskimi is working on and how

UID 2.0 integration

UID 2.0 Integration: A User Manual for Programmatic DSP

UID 2.0, also known as the Universal ID 2.0, is a collaborative initiative within the advertising industry designed to address the challenges of a cookie-less web, especially with the increased privacy regulations and browser restrictions. This manual focuses on integrating UID 2.0 into a programmatic Demand Side Platform (DSP) with emphasis on changes in audience sizes due to addressability restrictions on Safari and Firefox.

Introduction to UID 2.0

UID 2.0, or Universal ID 2.0, is an industry initiative designed as an alternative to third-party cookies for online ad targeting and tracking. Given the diminishing support for third-party cookies due to privacy concerns and browser restrictions, UID 2.0 uses various identifiers, from encrypted email addresses of users (with their consent) to 1st party cookies, as a basis for tracking and ad targeting. It aims to provide a standardised solution across the advertising industry that respects user privacy while still enabling targeted advertising.

Access on Safari and Firefox

With leading browsers like Safari and Firefox taking stringent measures against third-party cookies, advertisers and agencies have grappled with decreasing audience sizes and limited addressability. UID 2.0 offers a privacy-centric yet effective way to reach audiences on these platforms. **Eskimi** adoption of UID 2.0 means our partners can now connect with a previously untapped audience segment, making their campaigns more impactful than ever.

Benefits for Agencies and Advertisers:

1. **Enhanced Addressability**: Unlock precise targeting capabilities, ensuring that your brand message reaches the right audience at the right time, even on Safari and Firefox.
2. **Improved ROI**: Broaden your campaign reach to include engaged users on Safari and Firefox, leading to better conversions and improved return on advertising spend.
3. **Privacy-First Approach**: UID 2.0 still places user consent and privacy at the forefront. Advertise confidently, knowing you're compliant with the industry's latest privacy standards.

Redmob Data Legality, Validity & Security

DMP

Redmob DMP

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

Redmob DMP Data

Redmob 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. Redmob 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.

Redmob DMP Collection Schema

Redmob 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. Redmob DSP sends eligable data from the ad signal Redmob 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 Redmob DMP has collected.

Legal, Valid & Secure Data

Aktyvus sektorius UAB, doing business as Redmob, as a global provider of digital advertising media and data management technology. In our activities, Redmob 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?

Redmob 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 Redmob 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 Eskimi.*

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

More about Redmob Privacy Policy: https://www.redmob.io/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 Redmob 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.

Redmob 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 Redmob works with ensures the legality of the data that is sent to Redmob - including ways in which data is gathered and processed. Examples of processes are:
* Transaction validation. Every impression that comes between Redmob 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 Redmob 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 Redmob 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