
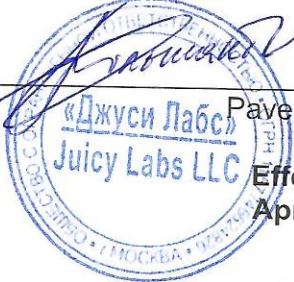


Approved by  
Administrative Order №47  
Dated April 27, 2024  
LLC "Juicy Labs" Director General

  
Pavel Bolshakov  
  
Effective date  
April 27, 2024

## DATA POLICY

## Table of content

### **1. General Provisions**

### **2. Terms and Definitions**

### **3. User Data Processing**

3.1. User Data Processing Purposes

3.2. User Data Processing Principles

3.3. User Data Categories

3.4. User Data Access

3.5. User Data Use and Disclosure

3.6. User Data Use Limitations

3.7. User Data Certain Categories Use and the Policy Application in Various Jurisdictions

3.8. Characteristics of Sessions Generated in Service Operation

3.9 Virtual Users Notification

3.10. User Data Erasure

### **4. Personal Data Processing**

4.1. Purposes of Personal Data Processing

4.2 Data Subjects

4.3. Legal Basis of Personal Data Processing

4.4. Data Subject Rights

4.5. Personal Data Erasure

### **5. Tracking Technologies**

5.1. Technologies used on Company's Website

5.2. Technologies used for Customer's/ Licensee's Personal Account functionality

5.3. How to delete Cookies from your browser?

### **6. Data Storage and Protection**

6.1. Personal Data and/or User Data Protection Measures

6.2. Personal Data and User Data Storage

### **7. Contact Us**

## 1. General Provisions

**Data Policy (hereafter «the Policy»)** is the present document, describing Virtual Users' User Data processing order, carried out by the Company during rendering services on fraud risk and other operational risks identification for the purpose of financial, reputational and other losses reduction for Customer's and Licensee's businesses and services, carried out online via the Internet. It also describes the Company's policy towards Personal Data Processing and discloses the information about the measures taken in the Company in order to ensure Personal Data security for protection of human and civil rights and liberties during one's Personal Data Processing, including protection of rights to privacy and private life.

The Policy is valid from April 27, 2024.

If there is no interpretation of the term used in "Terms and Definitions" section, the interpretation of the term, if necessary, is carried out in accordance with the Legislation.

### **Policy application and limitation of liability of the Company**

This Policy applies to the Company software use released in the last 6 (six) months for front-end/data collection and testing libraries and 36 (thirty-six) months for back-end/scoring libraries. We constantly notify Customers/Licensees of the necessary updates and provide all necessary materials and assistance, including automatic update mechanisms for front-end libraries.

We reserve the right to modify the present Policy anytime.

We kindly ask you to look through all the updates of our Policy on a regular basis.

## 2. Terms and Definitions

- **Authentication** is a process of Virtual User or/and Virtual User Device probabilistic fingerprinting (digital ID) via analysis of User Data and comparison of User Device data and/or Virtual User with a set of different attributes and characteristics in order to identify fraud or other operational risk, which may lead to financial, reputational or other losses of the Customer or Licensee, without the

use of Direct Identifiers and with the identifiers, which does not allow to identify the Virtual User.

- **Company (LLC «Juicy Labs», we)** is a legal entity registered in accordance with the legislation of the Russian Federation, MSRN 1157746624826.
- **Company's Feedback Form** is an application form placed on Company's Web Site designed for sending the requests to the Company from legal and natural persons regarding different cooperation issues.
- **Company's Web Site** is a web site generally available through the link <https://juicyscore.online/>, rights to the web site belong to the Company. The web site is used for the posting of content about Company's products and services for informational and other purposes.
- **Cookie** is a file, which usually consists of letters and numbers, located on the Device and/or transmitted from server and loaded to the browser's memory in the moment of submission or/and processing of the web site content. Cookie files allow the web site to identify the device of site visitor.
- **Customer or Licensee** are legal entities or individual entrepreneurs, to whom the Company provides services under the contract and/or provides the license for the Service.
- **Data Subject** is directly or indirectly identified or identifiable natural person.
- **Device** is a mobile or stationary device with an Internet access used by a Virtual User to enter Web Resource.
- **Direct Identifier** is a unique data attribute related to the Data Subject, which allows setting a univocal correspondence between the attribute and natural person.
- **Do Not Track** is a HTTP-headline, which notifies whether a Virtual User informs about one's willing/denial of tracking or monitoring of his actions on web sites or mobile application.

- **Identification** is a processing of natural person's Personal Data in order to identify the attributes, which individually or collectively let to identify this natural person clearly and unambiguously.
- **Irreversibly Changed Value** means a value obtained by irreversibly removing part of the original information and then hashing the rest of the information before analytical processing to avoid the possibility of restoring the original value.
- **JavaScript** for the purposes of the present Policy is a software, based on the relevant programming language and included to the Service for User Data collection via Web Resource.
- **Legislation** means a body of laws in force and applicable on the territory of the Russian Federation, which determines the cases and special aspects of the Personal Data and other data processing, as well as establishes requirements for the processing of Personal Data and other data.
- **Modified Value** is a value altered on Device by adding of dynamic variable alphanumeric character set and hashing; all alterations are performed before value processing by the Company software.
- **Natural Non-Randomness** is a nonzero probability of randomly guessing a natural person.
- **Personal Account** is a functionality within the secured part of the Services which is created for the Customer by the Contractor and allows receiving various technical information, statistics, and monitoring requests processing.
- **Personal Data** is any information relating to an identified or identifiable natural person (Data Subject).
- **Personal Data Processing** means any operation or set of operations which is performed on Personal Data, whether or not by automated means, including collection, recording, systematization, accumulation, storage, validation (update or alteration), retrieval, use, transmission (distribution, submission, access), anonymization, blocking, erasure or destruction.
- **SDK** in the present Policy means a software, based on the relevant programming language and included to the Service for User Data collection from iOS and

Android-family Devices via native mobile application of a Customer or a Licensee, as well as via mobile application JS App — Device Risk Analytics.

- **Service** means combined elements of the infrastructure, server hardware and software of the Company, which allow to estimate the risk of fraud or other operational risks of a Customer's or a Licensee's User formalized actions on the basis of User Data that do not allow to identify the User directly or indirectly.
- **Session (or JuicySession)** is a unique identifier of Internet-session (which is not Direct Identifier), registered on a Web Resource which is formed on the Company's servers and which is practically an enhanced token and does not contain Personal Data.
- **Soliciting Activity** means measures aimed at receiving and processing of consumers' requests for obtaining goods and services.
- **Unrecoverable Value** means the value obtained by irreversibly removing of a part of the original information and further hashing of the rest of information before analytical processing to avoid the possibility of restoring the original value.
- **User Data** is a Web Resource Virtual Users' data, collected by means of program modules, which neither contain Direct Identifiers, nor allow to identify a natural person directly or indirectly without the use of data not collected using Service main functionality.
- **Virtual User (User)** is a user of Web Resource of a Customer or a Licensee, which User Data is collected from correspondent Web Resource.
- **Web Resource** is a website, mobile application or any other resource of a Customer or a Licensee, which Virtual User may have access via the Internet.

### 3. User Data Processing

#### 3.1. User Data Processing Purposes

The Company performs processing of Virtual Users' User Data received from the Web Resources for specific purposes achievement, determined in advance by Customers or Licensees and under assignment of a Customer or a Licensee.

The Company processes User Data during services rendering to a Customer or providing the license to a Licensee by means of Device Authentication with the aim of fraud risk or any other operational risks assessment, which may lead to financial, reputational or any other losses of a Customer or a Licensee or/and of a Customer's or a Licensee's clients, to whom the services of a Customer or a Licensee are being provided via online channel through the Internet, as well as using online to offline principle (mobile application - JS App — Device Risk Analytics).

### **3.2. User Data Processing Principles**

User Data may be used in order to provide services by the Company to a Customer or in order to provide the license to a Licensee for fraud risk or any other operational risks assessment which may lead to financial, reputational or any other losses of a Customer or a Licensee or/and of a Customer's or a Licensee's clients, to whom the services of a Customer or a Licensee are being provided via online channel through the Internet;

The list of User Data categories processed by the Company is provided herein, open-ended, available for downloading and familiarizing, it contains parameters of the Device, software, network connection, not prohibited by configurations and settings of software;

Service functioning **does not imply** Personal Data Processing (such as natural person's full name, contact data such as full registered address, full mobile or phone numbers, email address, ID card or other personal documents data, as well as sensitive data as disposable income, expenses amount, confession, etc.). Personal Data are not required by the Company for the work of Service, shall neither be required by the Company nor provided by a Customer or a Licensee under the service contract or license contract;

User Data Processing corresponds to User safety principles during working online and to Apple and Google application development standards;

The Company does not collect or process Web Recourses Virtual Users' User Data, which infringe their fundamental rights and freedoms;

The Company processes User Data from Web Resources only under formalized confidential agreement or/and service agreement (contract) or license agreement (contract), negotiated and concluded by Customer's or Licensee's authorized representatives;

The Company does not process User Data for Virtual Users Identification and does not intend to do it in the future in order to minimize risks of the Virtual Users' rights and freedoms infringement as well as to increase value of User Data Processing as an alternative of Personal Data Processing.

Definitions of "User Data" and "Personal Data" as they stipulated hereabove are used for the purposes of the Policy. These definitions might have other meanings in different legal jurisdictions. Therefore, the Company recommends to Customers and Licensees prior to the Service use commencement to analyze and perform the necessary independent legal expertise for assessment of the Policy compliance with applicable law in order to meet requirements for information distribution, Users' consents collection and storage applicable in such legal jurisdiction.

### **3.3. User Data Categories**

The Company processes the following categories of User Data

- Collected by JavaScript (for web applications of a Customer or a Licensee, occasionally - for Customer's or Licensee's mobile applications) and SDK (for native mobile application of a Customer or a Licensee):
  - General data related to a Customer or a Licensee, their Web Resources and activity of the User on the Web Resource;
  - Conditions and circumstances of formalized actions performed on Customer's or Licensee's Web Recourses;
  - Device technical characteristics data (for example, Device make and model, screen size, memory capacity etc.);



- Device basic software data (for example, type and operating system version, browser type and version etc.);
- Internet-connection data being used by a Device at the moment when a User is on a Web Resource (for example, the category of IP address used, Internet connection speed);
- Data related directly to the Virtual User (for example, UserAgent and any other fields of web session header);
- Statistical data about Virtual User activities on the Web Resource (for example, the time when a User is on the Web Resource, the number of corrections made during the application form filling on Web Resource);
- Statistical data about the history length and URL, previous page, where the JavaScript is installed on Device;
- Statistical data about the categories of mobile Device applications (only via SDK);
- Statistical data about Device physical recourses utilizing level;
- Statistic data about Device graphic files (only via SDK);
- Data connected with Virtual User geographical location oversimplified to 1000 (one thousand) meters (only via SDK);
- Modified Device MAC-address (only via SDK). This attribute is not available for all integrations using an SDK version released by the Company after September 2023. For SDK versions that were released before the end of September 2023, this attribute collection and processing are **disabled by default**; such SDK versions are no longer supported by the Company. Customers are recommended to update integrations to actual versions. If Device MAC-address is necessary for the operation of the Customer's or Licensee's mobile application, then the collection and processing of this parameter may be included in order for the execution of agreements concluded only with those Customers/Licensees who did not update the SDK libraries used after September 2023, until the libraries update or until

the expiration of the library support period specified in Section 1 of this Policy; check applicable laws to avoid possible collection of Personal Data. Processing of this parameter cannot be enabled at the option of the Customer/Licensee;

- Modified MAC-address of Wi-Fi router (disabled by default). Collection and processing of this attribute may be enabled upon Customer's / Licensee's discretion for agreement execution, if such collection and processing do not infringe Virtual User's rights and freedoms and if the processing of this attribute is not recognized as the processing of personal data in jurisdiction of a Customer / Licensee;
- Typing rhythmical recurrence (collection and processing is **disabled by default**). If typing rhythmical recurrence dataset is required for Web Resource operation and the attribute processing does not infringe the rights and freedoms of a Virtual User and if the processing of this attribute is not recognized as the processing of personal data in accordance with the standards established by personal data laws and regulations in the jurisdiction of a Customer or a Licensee, taking into account the purposes of data processing, then collecting and processing of this attribute may be enabled at the discretion of a Customer or a Licensee;
- Alternative tracking technologies constituting IndexedDB persistent sessions. If a Customer or a Licensee needs to disable this functionality, a Customer or a Licensee shall follow the instruction contained in Company's technical manual;
- Modified Device ID value (only via SDK);
- Statistic and binary parameters of collateral activity performed on Device during online session.
- Collected from mobile User Device by mobile application JS App — Device Risk Analytics and by mobile SDK JuicyScore:

- Statistical data about Virtual User activities on the Web Resource (for example, the time when a User is on the Web Resource, the number of corrections made during the application form filling on Web Resource);
- Internet-connection data being used by a Device at the moment when a User is on a Web Resource (for example, the category of IP address used, connection speed);
- Device technical characteristics data (for example, Device make and model, screen size, memory capacity etc.);
- Data related directly to the Virtual User (for example, UserAgent and any other fields of web session header);
- Device basic software data (for example, type and operating system version, browser type and version etc.);
- Application identifier;
- Rough location data, related to Virtual User geographical location, oversimplified to 1000 (one thousand) meters;
- Selective list of applications installed;
- Device memory data;
- SIM-card data (to the exclusion of mobile number and SIM-card serial number);
- Host name;
- Device identifier (modified MAC-address). This attribute is not available for all integrations using an SDK version released by the Company after September 2023. For SDK versions that were released before the end of September 2023, this attribute collection and processing are **disabled by default**; such SDK versions are no longer supported by the Company. Customers are recommended to update integrations to actual versions. If Device MAC-address is necessary for the operation of the Customer's or Licensee's mobile application, then the collection and processing of this

parameter may be included in order for the execution of agreements concluded only with those Customers/Licensees who did not update the SDK libraries used after September 2023, until the libraries update or until the expiration of the library support period specified in Section 1 of this Policy; check applicable laws to avoid possible collection of Personal Data. Processing of this parameter cannot be enabled at the option of the Customer/Licensee;

- Modified MAC-address of Wi-Fi router (disabled by default). Collection and processing of this attribute may be enabled upon Customer's / Licensee's discretion for agreement execution, if such collection and processing do not infringe Virtual User's rights and freedoms and if the processing of this attribute is not recognized as the processing of personal data in jurisdiction of a Customer / Licensee;
- Wi-Fi connection information;
- Internet connection information;
- Bluetooth data (data whether Bluetooth is switched on or off are collected by default, other data collection is **disabled by default**, verify local legislation to enable this attribute);
- Battery data;
- Mobile service provider data;
- Information about volume of data transferred;
- Modified Device ID value (only via SDK and mobile application);
- Statistic and binary parameters of collateral activity performed on Device during online session;
- modified part of the Bonjour protocol configuration data (Zero Configuration Networking protocol - "working on a network with zero configuration");
- Information on KeyChain use.

### **3.4. User Data Access**

A Customer or a Licensee gets access to the User Data only through a request from information systems of a Customer or a Licensee via secure communication channels using an account created by the Company for a Customer or a Licensee on the basis of a confidentiality agreement, a service agreement or a license agreement previously signed by both parties.

### **3.5. User Data Use and Disclosure**

User Data disclosure occurs through sending the request from Customer's or Licensee's infrastructure to Company's infrastructure in accordance with the technical format of interaction.

The response to the request is an API Service answer, provided to the Customer or Licensee on the basis of signed agreement (contract) on behalf of both parties respectively.

The response to the request, above all else, contains the information, collected from Web Resources of a Customer or a Licensee as well as statistic data about visiting by the Virtual User of Web Resources of other Customers or Licensees of the Company. Source data are not transferred explicitly.

Data disclosure otherwise than due to service rendering to a Customer or providing a license to a Licensee by the Company in a specified format is not provided and prohibited.

In case if a Company identifies User Data, processing of which separately or collectively infringes Users' rights and freedoms, and (or) is considered as personal data processing under applicable law, and (or) User Data contains User's Direct Identifiers processing of such User Data shall be terminated and all the related User Data shall be deleted.

The Company shall not be liable for use or non-use of data, disclosed within the course of service rendering or license providing to a Customer or a Licensee respectively. Such data use or non-use is the sole liability of a Customer or a Licensee.

### **3.6. User Data Use Limitations**

User data SHALL NOT be used for purposes of active target marketing in order to attract clients to services and products of a Customer or a Licensee (the so-called «audience segmentation») as well as for any other purposes of Soliciting category contrary to the Principles of User Data Processing and inconsistent with the purposes of User Data Processing, established by the present Policy. Using the results of the Service in violation of this restriction is unacceptable and prohibited, since it violates the provisions of this Policy, the terms of the contract for the provision of services or a license contract concluded with a Customer or a Licensee, respectively, and also may be a violation of applicable law, depending on the jurisdiction of a Customer or a Licensee.

The Company does NOT process User Data, which let to identify Virtual User.

In the course of its main activity on informational services rendering or/and licensing the Company DOES NOT enrich and does not intend to enrich User Data by means of Personal Data in order to avoid the occasion of Virtual Users Identification.

### **3.7. User Data Certain Categories Use and the Policy Application in Various Jurisdictions**

Customers and Licensees are strongly recommended to validate the requirements of the Service and the collected data against compliance with the requirements of their applicable (local) laws and regulations.

If the applicable laws and/or the classification of data and/or associated risks adopted by a Customer or a Licensee categorizes all User Data obtained online as personal data (including the category of sensitive personal data), then a Customer or a Licensee shall, according to regulatory requirements, confirm the availability of all necessary consents of Data Subjects, the security of data processing and compliance with other mandatory requirements (technical details on cloud data processing are available upon request).

If a Customer or a Licensee identify a risk in the use of certain data/parameters collected within the Service and cannot disable the collection/processing of such parameters, in this case it is necessary to contact the Company's service department with a request to create the appropriate option (we will try to take into account the wishes within the Company's SLA).

In the event that a Customer or a Licensee conducts an independent technical audit of this type of parameters (data types) processing risk, it should be taken into account that the more audits are carried out, the more reasonable the assessment will be.

If a Customer or a Licensee identifies, in course of one of these audits, a risk that exceeds multiples of the existing level of Natural Non-Randomness, it is necessary to immediately provide us with a reproducible approach confirming this risk, and the Company will take immediate measures to eliminate the risk after it is confirmed.

While performing our main activities we have witnessed a number of specific regulations related to User Data usage in various legal jurisdictions. Therefore, we kindly ask you to pay your close attention to the following User Data in terms of sensitivity of the data or considering these parameters as personal data in accordance with applicable law:

- Internet connection basic data (these data points are always presented in the sessions of all the companies working online as the integral part of any internet connection);
- Modified Device MAC-address (only via SDK). This attribute is not available for all integrations using an SDK version released by the Company after September 2023. For SDK versions that were released before the end of September 2023, this attribute collection and processing are **disabled by default**; such SDK versions are no longer supported by the Company. Customers are recommended to update integrations to actual versions.
- Typing rhythmical recurrence (collection and processing options are **disabled by default**);

- Alternative tracking technologies constituting of IndexedDB persistent sessions. Despite of the incomplete match with Cookie of Document.Cookie, LocalStorage, SessionStorage sections persistent sessions are NOT available to the third parties and, as a rule, do not have unambiguous bijection between file (s) name (s) and session value, moreover, persistent session value is derived from the value of one of the online sessions for hedging of the risk of accidental occurrence of unauthorised data (for hedging of risk of values occurrence different from random set of numbers, letters and symbols and the time of session creating) in persistent session value. This type of data may be considered as Cookie in a range of jurisdictions.
- If User Data processing carried out solely to identify the risk of fraud and other operational risks, without additional data enrichment and without the possibility of direct Identification of the Virtual User, but associated with probabilistic User or Device Authentication, is considered as personal data processing in the legal jurisdiction of a Customer or a Licensee, then a Customer or a Licensee shall comply with requirements of applicable personal data legislation when handling such User Data and using the Service.

### **3.8. Characteristics of Sessions Generated in Service Operation**

Common Sessions are not stored on Virtual User's Device, they are stored only in Virtual User Device browser's memory.

The Session is created at the moment when a Virtual User enters Web Resource of a Customer or a Licensee on the servers within the Company's infrastructure basing on random number generator and the moment of referencing of Company's infrastructure. For that reason, Sessions cannot serve as Direct Identifiers of a Virtual User.

Session Identifier depends on random number generator as well as on the moment of referencing to service and is similar to a random enhanced token,



which is created for online payments and does not depend on User or User's Device.

Sessions are not synchronized with 3rd parties' sessions. Virtual Users' Data is not enriched with 3rd parties' data, including Virtual Users behaviour on the other internet resources beyond the frames of Company's Service activity.

Basing on the objectives of automated collection of User Data, value of flag Do Not Track is not taken into account during Sessions and data collection program modules operation, operating on a Web Resource.

### **3.9 Virtual Users Notification**

In accordance with the applicable law on personal data, a Customer or a Licensee is obliged to notify Virtual Users of their Web Resources about Sessions generated by the Company and operating on those Web Resources, as well as about automatic collection of User Data by means of program modules, provided by the Company. Virtual User notification shall take place prior to the data collection commencement.

In order to assist to Customers or Licensees in Virtual Users notification the Company adds the paragraph to the service contract or license contract related to notification of Users.

The Company recommends to use the following notification template to notify Virtual Users — visitors of Web Resources.

"The company LLC «Juicy Labs» (OGRN 1157746624826, INN 7717 294300), registered at the address 15A, Leninskiy Avenue, Intracity Territory Municipal District Donskoy, Moscow 119071, Russia, email address info@juicyscore.com performs collecting, processing (including storage, systematization, accumulating, analysis, update, extraction and deletion) of user data by means of JavaScript <for the web application of a Customer or a Licensee> and SDK <for a native mobile application a Customer or a Licensee> on the web resource <the name of a Web Resource of a Customer or Licensee> in order to assess risks of the application for a Customer's or Licensee's product obtaining under assignment

of a Customer or a Licensee. The list of user data as well as its content, storage and deletion procedures are given in Data Policy, available on the web site [https://juicyscore.online/en/privacy/»](https://juicyscore.online/en/privacy/).

Customers and Licensees conducting business in EU jurisdiction shall notify their Users about Device fingerprinting mechanisms and/or external sessions running on their Web Resources. This notification shall appear before Users enter the page(s) created with mentioned mechanisms and/or containing mentioned sessions. JuicyScore data collector (JavaScript) is recommended for installation on User's Web Resource starting from the second page (not landing page); JuicySessions should be classified as essential Cookies or as other obligatory data category since the Sessions are not Cookies and are not files and are stored in web browser short-term memory. Virtual User's decline of such Sessions use should be treated as a decline of continue Web Resource visit.

### **3.10. User Data Erasure**

Since User Data collected and processed within the Company's infrastructure and may not be classified as Personal Data, deletion of such data under User's request is possible only in theory, because there is no such option to bind technical data collected by the Company to User's Personal Data on the side of a Customer or a Licensee.

Submission User Data deletion application is available:

- Via the feedback form on the Company's Web Resource ([www.juicyscore.online](http://www.juicyscore.online)) in English,
- Via written request, send to the address: 15A, Leninskiy Avenue, Moscow 119071, Russia.

The Company commits to take all possible measures to implement received applications on User Data deletion. The application lead time does not exceed 30 (thirty) calendar days from the moment of application submission.

## **4. Personal Data Processing**

### **4.1. Purposes of Personal Data Processing**

The Company is an Operator with respect to Personal Data of Data Subjects specified in clause 4.2 herein.

Personal Data Processing is limited by achievement of specified, explicit and legitimate purposes.

The content and scope of the processed Personal Data correspond to the stated purposes of processing. The Personal Data shall be adequate, relevant and comply with the stated purposes of processing.

Personal Data Processing incompatible with the purposes of Personal Data collection is not allowed.

The Company does not process Personal Data during service rendering to a Customer or during the license providing to a Licensee.

The Company processes Personal Data for the following purposes:

- Signing a contract with Data Subject and its further performance;
- Conducting Company's personnel management and record keeping;
- Corporate documentation and records maintenance in accordance with the legislation of Singapore, recruitment;
- Conducting economic and administrative activities;
- Contact with the representatives of legal entity which is a potential user of Company's services, advice on services, rendered by the Company;
- Entering into and performance of the service agreement or license agreement;
- Other legitimate purposes, provided for by applicable law.

## **4.2 Data Subjects**

The Company processes Personal Data of the following categories of Data Subjects:

- Natural persons, who are job candidates;
- Natural persons, who are Company's founders or employees;
- Natural persons, who are dismissed employees;
- Natural persons, carrying out work under a contract with the Company;
- Natural persons, who left one's request in a feedback form on the Company's Web Site;
- Natural persons, who are contact persons of the companies – parties of the contracts executed;
- Any other natural persons, provided consent for Personal Data Processing by the Company.

## **4.3. Legal Basis of Personal Data Processing**

The Company processes Personal Data in strict compliance with the applicable law.

Personal Data Processing shall be lawful only if and to the extent that at least one of the following applies:

- the Data Subject has given expressed consent to the Personal Data Processing for one or more specific purposes;
- Personal Data Processing is necessary for the performance of a contract to which the Data Subject is a party, or a beneficiary, or a guarantor as well as for execution of a contract initiated by Data Subject or a contract under which Data Subject will be the beneficiary or guarantor. The contract concluded with Data Subject shall not contain provisions restricting the rights and freedoms of Data Subject, establishing the cases of processing

minors' personal data of minors, unless otherwise provided by the Legislation, as well as provisions that allow Data Subject omission as a condition of the conclusion of the contract;

- Personal Data Processing is necessary for compliance with a legal obligation to which the Company is subject;
- Personal Data Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party, or to achieve socially significant goals subject to non-infringement of fundamental rights and freedoms of Data Subject.

#### **4.4. Data Subject Rights**

The Data Subject has the right to:

- Obtain the information related to one's Personal Data Processing in order, form and terms set by Personal Data regulations;
- Require: rectification of Personal Data; blocking or erasure of Personal Data if such Personal Data are incomplete, outdated, unreliable, illegally received, not necessary for the purpose they were collected for or used for purposes not stated at the moment of Data Subject content;
- Take the measures prescribed by law in order to protect one's rights;
- Withdraw a consent to Personal Data Processing;
- Exercise any other rights provided for by the personal data legislation.

#### **4.5. Personal Data Erasure**

Personal data Erasure is available through application submitted:

- Via feedback form on the Company's Web Site ([www.juicyscore.online/en](http://www.juicyscore.online/en)) in English;

- Via the request in written form, send to the address 15A, Leninskiy Avenue, Moscow 119071, Russia.

The Company commits to take all possible measures in order to implement the received applications to delete the Personal Data. The Company shall erase such Personal Data during the term not exceeding 7 (seven) business days from the date of submission by the Data Subject or his/her representative of information confirming that such Personal Data are illegally obtained or are not necessary for the stated purpose of processing. The Company is obliged to notify Data Subject or his/her representative of the changes made and the measures taken and take reasonable measures to notify third parties to whom the Personal Data of such Data Subject were transferred.

Personal Data is to be erased upon reaching the purposes of Personal Data Processing or in case of Data Subject consent withdrawal of Personal Data Processing, provided that:

- It has not been otherwise agreed in the contract, a party and beneficiary and guarantor of which is the Data Subject;
- The Company has no right to process Personal Data without the Data Subject consent pursuant to national personal data legislation;
- It has not been otherwise stated by any other agreement between the Company and Data Subject.

## **5. Tracking Technologies**

### **5.1. Technologies used on Company's Website**

We use various tracking technologies on Company's Web Site, such as scripts for collection and processing of information related to Web Site visitors while they stay on the Web Site, such as IP address, location (country or city), type and version of Device operating system, type and version of Device browser, type and resolution of the display, source of traffic, operating system and browser language and others.

Cookies are not used on the Company's Web Site in the meaning of files, stored in the relevant section Document.Cookies, LocalStorage, SessionStorage of browser database. Alternative tracking technologies are not used on the Company's Web Site, such as persistent sessions in IndexedDB, Device Fingerprinting, ETag marks.

We may use a variety of online analytics products that use Cookies to help us analyze how Users use the Web Site and Services and enhance your experience when you use the Site and Services.

Types of tracking technologies used on the Company's Web Site:

- IndexedDB, storage period is constantly. This method of persistent sessions use is set up on the feedback form in order to enable data deletion upon request;
- Device Fingerprinting, storage period is 3 months. Device Fingerprinting mechanism is set up on the feedback form in order to enable data deletion upon request. In the SDK settings, it is possible to disable Device Fingerprinting tools that are based on graphics and media and are different from the basic ones accepted in the financial sector, as well as to disable different types of Device Fingerprinting formed on the Virtual User's Device (for a more detailed description, please refer to the Company's technical documentation provided during the execution of the agreement concluded with the Customer/Licensee).

Please note that the use of User Data solely to identify the risk of fraud or other operational risks in order to reduce financial, reputational or other losses for the businesses and services of the Customer or the Licensee, as well as for security purposes, is not regarded by the Company as tracking, therefore the value of the Do Not Track flag is not taken into account during the operation of Sessions and data collection software modules running on the Web Resource.

If the storage of constant session (persistent session) in browser memory of User's Device infringes requirements of personal data legislation established in legal jurisdiction of a Customer or a Licensee, this technology may be disabled.

## **5.2. Technologies used for Customer's/ Licensee's Personal Account functionality**

The Company uses Cookies to maintain the operation of the Customer/Licensee's Personal Account, created for interaction with the Customer/Licensee under the concluded agreement. At the same time, the Customer/Licensee is required to obtain the consent of individuals whose contact details are indicated in agreement with a Customer / Licensee and who interact with the Company through the Personal Account to process personal data and transfer such data to the Company in order to fulfill obligations under concluded contracts.

For Customer's / Licensee's Personal Account protection persistent sessions (IndexDB and Device Fingerprinting) are applied, application instructions are described in clause 5.1 herein.

## **5.3. How to delete Cookies from your browser?**

You can withdraw your consent to Cookies storage by changing your browser settings.

You can find the instructions about Cookies management, published by providers of Microsoft Edge, Google Chrome, Safari (for computers, mobile devices), Firefox, respectively.

# **6. Data Storage and Protection**

## **6.1. Personal Data and/or User Data Protection Measures**

The Company takes all the necessary legal, organizational and technical measures in order to protect data collected from unauthorized, illegal or accidental access, deletion, changing, blocking, copying, providing, distribution of data, to which may refer:

- Limitation and regulation of the staff, who has access to the Personal Data and/or User Data via the Feedback form on the Company's Web Site;



- Designation of a person responsible for organization of Personal Data and/or User Data Processing; designation of a person responsible for security of Personal Data or/and User Data;
- Familiarization of employees who are directly in charge of Personal and/or User Data processing with the provisions of the applicable legislation and this Policy;
- Organization of accounting, storage and circulation of media, which contain the information about Personal and/or User Data;
- Identification of threats to Personal Data security during its processing, threat models developing;
- Personal Data protection system development on the basis of threat models;
- Testing of readiness and effectiveness of the information security tools use;
- Separate access of users to the informational resources, software and hardware information processing tools;
- Registration and accounting of information systems users' activities;
- Information system access password protection;
- Physical division of Personal Data and User Data storage and processing systems and preventing of combined storage, processing or/and any other activities;
- Application of instruments for control of access to communicational ports, output information devices, removable media as well as external memories;
- Antivirus control; application of firewall; information backups;
- Provision of data recovery, modified or deleted in the result of illegal access.

## **6.2. Personal Data and User Data Storage**

Personal Data storage is carried out in a manner that allows to identify the Data Subject and for a period no longer than it is required for the purposes of Personal Data Processing unless otherwise provided for by applicable personal data legislation. The terms of Personal Data storage are established subject to compliance with requirements of personal data legislation or provisions of a contract, party and beneficiary or guarantor of which is the Data Subject. Personal Data is to be deleted after the expiration of the storage period.

User Data collected from Web Resource, in respect of which there was NO request to the Service for User risk assessment from a Customer or a Licensee, is stored for not more than 30 (thirty) days from the moment of collection.

User Data collected from the Web Resource in respect of which there was a request from a Customer or Licensee for User risk assessment, is stored for not more than 2 (two) years from the moment of collection.

All the raw data, including User Data, are localized in the regions of the use of Service (determined on the basis of Virtual User IP address location) in order to comply with applicable legislation or/and current business practices and regulations. For data storage the Company uses physical infrastructure, situated in the regions of the Service use. Localization is set by default taking into account proximity of Virtual User IP-address to data storage physical infrastructure, if other localization set is not forced by a Customer of a Licensee.

The Company is not the owner of User Data, processed in Company's IT-systems and provides its secure storage basing on the service contract, signed with a Customer or license contract signed with a Licensee.

## **7. Contact Us**

LLC «Juicy Labs» (MSRN 1157746624826, TIN 7717294300)

Registered and mailing address: 15A, Leninskiy Avenue, Intracity Territory Municipal District Donskoy, Moscow 119071, Russia.

E-mail address for messages on Personal Data Processing and User Data issues:  
[info@juicyscore.com](mailto:info@juicyscore.com).

Phone: +7 (495) 532 3999.