DATA POLICY

I. LIST OF TERMS AND DEFINITIONS

1. Authentication is a process of probablistic fingerprint (digital ID) identifying of Virtual user or/and Virtual virtual user 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 determine operational or other financial risk without the use of direct identifiers and with the identifiers, which does not allow to identify the Virtual user.
2. Web resource is a web site, mobile application or any other resource, which Virtual user (or a User) can access via the Internet.
3. Virtual user (User) is a user of web resource of a Customer or Licensee, in respect of which the User data is collected being the result of any of user's acts performed on the web site or mobile application.
4. 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.
5. 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.
6. The company (Juicy Labs LLC, we) is a legal entity registered in accordance with the legislation of the Russian Federation at the address Moscow, Bolshaya Gruzinskaya str., 30A bld. 1, 4th floor, office 413.
7. Login of an e-mail address have the form of latin characters, numbers and reserved characters combination, preceding the sign @ («at») in the e-mail address name.
8. Unrecoverable value in the Policy means that the primary e-mail Login value is reduced by 5 symbols on average depending on the length of the reference value and minimum by 2 symbols before analytical processing in order to avoid the occasion of reference value rollback.
9. Personal data processing: any action (operation) or cumulative actions (operations) with Personal data, carried out by means of automation techniques or without the use of such techniques.
10. Obfuscation stands for converting of the source text or executable code of the program to a form that preserves its functionality and reduces the size of the executable program file.
11. Personal data is any information related directly or indirectly to a determined or determinable natural person (subject of personal data).
12. User data is data on Web resource Virtual users collected by means of program modules, using these program modules it is impossible to determine a natural person.
13. Direct identifier is a unique data attribute related to the data subject, which allows making an univocal correspondence between the attribute and natural person.
14. Company's web site is a public web site available through the link https://juicyscore.com/, 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.
15. Service: combined elements of the infrastructure, server hardware and software of the Company, which allow to estimate operational Customer or Licensee User application risk on financial products basing on User data, which does not allow to identify the user directly or indirectly.
16. Session (or JuicySession) is a unique identifier of Internet-session, registered on a web resource of a Customer or Licensee which is formed on the Company's servers and which is practically an enhanced token and does not contain Personal data.
17. Device is a mobile or stationary device with an Internet access used by a Virtual user to enter a Client's or Licensee's web resource.
18. The Company's feedback form: The Company's application form placed on Company's public web site designed for sending the requests to the Company from legal and natural persons regarding different cooperation issues.
19. 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.
20. 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.
21. JavaScript: in terms of the present Policy is a software, based on the relevant programming language and included to the Service for User data collection via web application of a Customer or Licensee.

22. SDK in terms of the present Policy is a software, based on the relevant programming language and included to the Service for User data collection from IOS and Android devices via native mobile application of a Customer or Licensee.
23. Soliciting activity — measures aimed at receiving and processing of consumers' requests for obtaining goods and services.

II. GENERAL PROVISIONS

Data Processing Policy (hereafter «the Policy») describes Virtual users' User data processing order, carried out by the company during rendering services on operational risks and fraud risks identification as well as operational and financial risks 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 order to ensure Personal data security in the Company to protect the rights and freedoms of a human and citizen during his personal data processing, including protection of rights to personal privacy and private life.

The current Policy is valid from 22.12.2022.

III. WHO WE ARE AND HOW TO CONTACT US?

E-mail address for messages on Personal data processing and User data issues: info@juicyscore.com.

LLC «Juicy Labs» (OGRN 1157746624826, INN 7717 294300), registered at the address Moscow, Russia, postal code 123056, Bolshaya Gruzinskaya str.30A, bld.1, office 413. Contact phone number: +7 (495) 532 3999.

«JUICYSCORE HOLDING PTE. LTD.» (UEN 202128709Z), registered at the address #10-01 ONE GEORGE STREET, SINGAPORE, postal code 049145 Contact phone number: +65 69786805.

IV. USER DATA PROCESSING

1. **User data processing purposes**

   Under assignment of Customers or Licensees the Company provides User data processing related to Virtual users from the Web resources of a Customer or Licensee guided by the achievement of specific purposes, determined in advance by Customers or Licensees.

   The Company processes User data in the provision of services to a Customer or providing the license to a Licensee by means of Virtual user device Authentication with the aim of fraud risk assessment or any other operational risks, which may lead to financial, reputational or any other losses of a Customer or Licensee or/and of the Customer or Licensee's clients, to whom the services of a Customer or Licensee are being provided via online channel through the Internet.

2. **User data processing principles**
   1. The 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 assessment or any other operational risks which may lead to financial, reputational or any other losses of a Customer or Licensee or/and of a Customer or Licensee's clients, to whom the services of the Customer or Licensee are being provided via online channel through the Internet;
   2. The list of categories of User data, processed by the Company is open-ended, available for downloading and familiarizing, it contains parameters of the Device, software, network connection, not prohibited by configurations and settings of software;
   3. Service functioning does not imply Personal data processing, Personal data are not required by the Company for the work of Service and won't be required by the company within the frames of the service contract or license contract;
   4. User data processing corresponds to the Code of ethical behaviour online, user safety regulations during working online and Apple and Google application development standards;
   5. The Company does not collect or process User data about Virtual users — web resources visitors of the Customer or Licensee, which discriminate against their rights and freedoms;
   6. The company processes User data from web resources of a Client or Licensee only on the basis of formalized confidential agreement or/and service agreement (contract) or license agreement (contract), negotiated and concluded by the authorized persons of Customer's or Licensee's Companies;
   7. 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 for the rights and freedoms of Virtual users as well as value addition to User data processing as an alternative of Personal data processing.
   8. Definition and interpretation of User and Personal data categories may differ depending on the jurisdiction of a Customer or Licensee. The company recommends to a Customer and/or Licensee to perform the necessary legal expertise at the beginning of the use of Service and to use the applicable interpretation of data with the necessary rules of information distribution, Users' consents collection and storage.

3. **What User data do we process?**

   The company processes the following categories of User data, collected by JavaScript (for web applications of Customer or Licensee) and SDK (for native mobile application of Customer or Licensee):

   1. General data related to a Customer or Licensee, their web resources and activity of the User on the web resource of a Customer or Licensee;
   2. Conditions and circumstances of form applications for financial products obtaining;
   3. Device technical characteristics (for example, device make and model, screen size, memory capacity etc.);
   4. The data about basic software of a device (for example, type and operating system version, browser type and version etc.);
   5. Internet-connection data being used by a device at the moment when a suer is on the Customer or Licensee's web resource (for example, the category of IP address used, connection speed);
   6. Data related to the Virtual user, for example, UserAgent and any other fields of web session header;

7. Statistical data about the activities of Virtual user on the web resource of a Customer or Licensee (for example, the time when a User is in on the web resource, the number of corrections made during the application form filling on web resource);
8. Statistical data about the history length and URL, previous page, where the JavaScript on Virtual user device;
9. Statistical data about the categories of mobile device applications (only via SDK);
10. Statistical data about geographical files of a device (only via SDK);
11. Data connected with geographical location of Virtual user, oversimplified to 1000 (one thousand) meters (only via SDK);
12. MAC-address (only via SDK, collection and processing turned off in default). If MAC-address is required for mobile application operation of a Customer or Licensee and the processing of this attribute does not break the rights and freedoms of Virtual user as well as meets the standards established within the jurisdiction of Customer or Licensee by the law about personal data taking into account the aims of data processing, then data processing and collecting of this parameter may be included at the discretion of Customer or Licensee.
13. Typing rhythmical recurrence (collection and processing option is disabled by default). If typing rhythmical recurrence dataset is required for web resource of the Customer or Licensee operation and the attribute processing does not violate the rights and freedoms of a virtual user and complies with the norms of the Customer or Licensee personal data legislation, collection and processing of this parameter may be enabled at the discretion of the Customer or Licensee.
14. Alternative tracking technologies constituting IndexedDB persistent sessions. If you need to eliminate this functionality, please follow the instruction contained in technical manual.
15. Modified device_id value (only via SDK, the value is modified on a device by adding dynamic salt and hashing; all the modifications occur until the moment of processing of the values within JuicyScore).

The JS App — Device Risk Analytics mobile app as well as JuicyScore mobile SDK are processing and collecting the following types of data:

1. Statistic data on Virtual user activity on Licensee or Customer web resource
2. Device internet connection data in the moment of user activity on Licensee or Customer web resource
3. Data related to a Virtual user
4. Device core software data
5. Application identifier
6. Coarse location
7. List of installed applications (this data type is excluded by default, please refer to the laws of your country)
8. Device storage information
9. Device SIM information (excluding phone number and SIM serial number)
10. Host name
11. Device ID (Mac address, this data type is excluded by default, please refer to the laws of your country)
12. Wi-Fi connection data
13. Internet connection data
14. Bluetooth data (by default the only data type collected is on/off radio state, for enabling other data types please refer to the laws of your country)
15. Battery data
16. Operator data
17. Data traffic statistics

4. **Limitations of User data usage:**
    1. User data MAY NOT be used for purposes of active target marketing in order to attract clients to services and products of a Customer or Licensee (the so-called «audience marking») as well as for any other purposes from «soliciting» category contrary to the Principles of User data processing and inconsistent with the aims of User data processing, established by the present Policy.

2. User data collected from web resource of a Customer or License, for which there was NO request to the Service from Customer or Licensee for User risk assessment, is stored for not more than 3 (three) months from the moment of collection;
3. User data collected from the web resource of a Customer or Licensee for 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;
4. The Company does NOT process User data, which let to identify Virtual user. If a Company gets the access to the information, which lets to identify Virtual user, then, in accordance with the data processing algorithm being used by the company at the moment, the company obfuscates or changes the fields up to Unrecoverable value either on Customer or Licensee's side, or during information processing by the Company;
5. Within the frames of the core activity to provide informational services or/and providing the license 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 accidental Virtual Users Identification.
6. While performing our core activities we have witnessed a number of notations related to user data usage in various jurisdictions. Therefore we kindly ask you to pay your close attention to the following user data in terms of sensitivity of the data or regarding these parameters as personal data:
   - 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);
   - MAC-address (only via SDK, collection and processing option is disabled by default);
   - Typing rhythmical recurrence (collection and processing option is disabled by default);
   - Irreversibly changed email login reduced by 5 symbols on average and minimum of 2 symbols (this parameter refers to virtual user sensitive data in a range of jurisdictions);
   - Alternative tracking technologies constituting of IndexedDB persistent sessions. Despite of the incomplete match with cookie-files 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 regarded as cookies in a range of jurisdictions.

5. **Characteristics of sessions generated within the work of Service:**

Common sessions are not stored on Virtual user device, they are stored only in browser's memory of Virtual user device.

The session is created in the moment when a Virtual user enters web resource of a Customer or 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 they can not be 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, level of flag Do Not Track is not taken into account during Sessions work and data collection program modules, operating on a Customer or Licensee's web resource.

6. **Dissemination of information to Virtual users**

In accordance with the personal data applicable law, a Customer or Licensee are obliged to inform Virtual users of their web resources about the operating sessions on those web resources, generated by the Company, as well as about automatic collection of User data by means of program modules, provided by the Company. Dissemination of information to Virtual user has to take place since the moment of data collection commencement.

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

The company recommends to use the following format of Virtual users notification — web resources visitors of a Customer or Licensee.

On the web resource in order to assess risks of the application for financial product obtaining of a Customer or Licensee under assignment of the Customer or Licensee the company LLC «Juicy Labs» (OGRN 1157746624826, INN 7717 294300), registered in Moscow, Russia, postal code 123056, Bolshaya Gruzinskaya str.30A, bld. 1, office 413, phone number +7 495 532-39-99, aemail address info@juicyscore.com is 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 Licensee) and SDK (for a native mobile application a Customer or Licensee). The list of user data as well as its content, storage and deletion procedures is given in Data processing policy, available on the web site juicyscore.com/ru/privacy».

7. **Deletion of User data**

Since User data, collected and processed within the Company’s infrastructure, may not be classified as Personal data, deletion of such data by user’s request is possible only in theoretical field, because there is no such option to bind technical data, collected by the Company, to Personal data of a User on the Company’s side.

Mechanism of making a request for User data deletion is available:

- Via the feedback form on the Company’s web resource (www.juicyscore.com) in English and Russian,
- Via the request in written form, send to the address Moscow, Russia, postal code 123056, Bolshaya Gruzinskaya str.30A, bld.1, office 413.

The company pledges to take all possible measures in order to implement the sent requests to delete the data. The term of consideration of applications does not exceed 30 (thirty) calendar days from the moment of request submission.

8. **The use and disclosure of User data**

Disclosure of User data occurs through sending the request from Client’s or Licensee’s infrastructure to Company’s infrastructure in accordance with the technical format of interaction.

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

The response format to the request, above all else, contains the information, collected from web resources of Client or Licensee as well as the data, received on the web resources of other Clients or Licensees of the Company, reflected in the form of statistic data about visiting of indicated web resources by the Virtual user.

Data disclosure otherwise apart from service rendering to a Client 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 discriminates the rights and freedoms of Users and (or) in terms of legislation is regarded as Personal data processing, processing of such User data is terminated immediately and all the related User data is deleted.

The use or non-use of data, disclosed within the frames of service rendering or license providing to a Customer or Licensee respectively is the responsibility of a Customer or Licensee — Company is not responsible for it.

V. PERSONAL DATA PROCESSING

1. **Purposes of personal data processing**

   LLC «Juicy Labs» is an operator within the frames of Personal data legislation.

   Personal data processing is limited by achievement of specific, determined in advance and legal purposes.

   The content and volume of personal data processed is in accordance with the stated purposes of processing. Personal data processed should not be excessive regarding 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 in providing the Service during service rendering to the Customer or during the license providing to the Licensee.

   The Company processes Personal data for the following purposes:

   - Signing a contract with personal data Subject and its further performing;
   - Conducting personnel work and Company's Employees' accounting management;
   - Maintenance of corporate documentation and records in accordance with the legislation of the Russian Federation, searching and selection of candidates for vacant position in the Company;
   - Conducting economic and administrative activities; conducting the contact with the representatives of organization — potential user of Company's services, advice on services, rendered by the Company; entering into the service agreement or license agreement; and also in order to achieve the goals, provided for by law.

2. **Whose Personal data do we process?**

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

   - Natural persons, who are candidates for a vacant position in the Company;
   - Natural persons, who are Company's founder or employees;
   - Natural persons, who are dismissed employees;
   - Natural persons, carrying out work under a civil contract with the Company;
   - Natural persons, who left one's request in a feedback form on the web site of the Company;
   - Natural persons, who are contact persons of the companies-clients, with whom the contracts are entered into;
   - Any other natural persons, who expressed the consent for personal data processing by the Company;

3. **Legal basis of Personal data processing**

   The Company processes personal data in strict compliance with the law.

   Personal data may be processes in the following cases:

   - The Subject of Personal data expressed consent for personal data processing for one or several purposes;
   - Processing is required in order to fulfill a contract, according to which the subject of Personal data is one of the parties, or in order to take measures on demand of the subject before making an agreement;
   - Processing is required for the implementation of legally binding obligations entrusted to the Company;
   - Processing is required in order to ensure legitimate interests of the Company or 3rd party except for the cases, when such interests are counter to the interest or general rights and freedoms of data subject, which require personal data protection, in particular, if the subject of personal data is a child.

4. **The rights of the Subjects of Personal data**

   The subject of Personal data has the right to:

- Acquire the information related to one’s personal data processing in order, form and terms set by personal data legislation;
- Require clarification of one’s personal data, its blocking or deletion in case if personal data is not full, outdated, untruthful, obtained illegally and is not necessary for the stated purpose of processing or is used in purposes, which have not been stated previously during the providing the consent to personal data processing;
- Take the measures prescribed by law in order to protect one’s rights;
- Revoke a consent to personal data processing;
- Any other rights prescribed by the Personal data legislation.

5. **Personal data deletion**

Personal data deletion is available:

- Via feedback form on the web resource of the Company (www.juicyscore.com) in Russian and English;
- Via the request in written form, send to the address Moscow, Russia, postal code 123056, Bolshaya Gruzinskaya str.30A, bld.1, office 413.

The company pledges to take all possible measures in order to implement the sent requests to delete the data. The term of consideration of applications does not exceed 30 (thirty) calendar days from the moment of request submission.

On reaching the purposes of personal data processing and in case of withholding the consent to personal data processing by the subject of Personal data, Personal data is to be deleted if:

- It has not been otherwise agreed by the contract, party and beneficiary and guarantor of which is the Subject of Personal data;
- The Company has no right to process personal data without the consent of Personal data Subject on grounds, prescribed by national Personal data legislation;
- It has not been set up by any other agreement between the Company and Subject of Personal data.

VI. TRACKING TECHNOLOGIES

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 operating system of your device, type and version of browser on your device, type and resolution of the display, source of traffic, operating system and browser language and others.

Cookies are not used on the web site in the meaning of files, stored in the relevant section Document.Cookies of browser database. Alternative tracking technologies are used on the web site, such as persistent sessions in IndexedDB, Device Fingerprinting, ETag marks.

Types of tracking technologies used on the Company’s web site:

- IndexedDB, storage period: constantly; This method of use of persistent sessions is set up on the feedback form in order to be able to delete data on request
- Device Fingerprinting, storage period: 3 months; Mechanism Device Fingerprinting is set up on the feedback form in order to be able to delete data on request

If the storage of constant session (persistent session) in browser memory of User’s device violates the rules of personal data legislation established within the jurisdiction of the Client or Licensee, this technology may be turned off.

What can you do if you want to delete cookie files from you browser?

You can withhold your consent to cookie files storage by changing your browser settings.

You can find the instructions about cookie files management, published by providers Google Chrome, Safari (for computers, mobile devices), Firefox, respectively.

VII. DATA STORAGE AND PROTECTION

1. **Data protection measures**

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

   - Limitation and regulation of the staff, who have access to the Data via the Feedback form on the Web resource of the Company;
   - Designation of a person responsible for organization of Personal data processing and/or Personal data; designation of a person responsible for security of Personal or/and User data;
   - Raising the awareness of the employees who are directly in charge of Personal and/or User data processing about the provisions of the applicable data legislation, including Personal, Present Provision; 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, formation of threat models based on them;
   - Development of the system of Personal data protection on the basis of threat models;
   - Checking the readiness and effectiveness of the use of information security tools;
   - Control of users access to the informational resources, software and hardware information processing tools;
   - Registration and accounting of informational systems users activities;
   - Password protection of the access to the information system;
   - Physical division of Personal data storage and processing systems or/and Personal data 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;
   - Administration of antivirus control; application of firewalling; information backups;
   - Provision of data recovery, modified or deleted in the result of illegal access to it.

2. **User data access**

   Access to User data is conducted by a Customer or Licensee only via making the request from informational system of a Customer or Licensee through secure channels of communication with the use of an account, provided to a Customer or Licensee by the Company basing on the service contract or license contract signed by both parties.

3. **Data storage**

   Personal data storage is carried out in a way, that allows to identify the Subject of Personal data for not longer that it is required for the purposes of Personal data processing, except for the cases, when the term of Personal tada storage is not estimated by federal law or a contract, party and beneficiary and guarantor of which is the Subject of Personal data. Personal data is to be deleted after the expiration of the storage period.

   All data, including Personal data, collected from Virtual users, is situated on the territory of Russia Federation (is determined on the basis of Virtual user IP address location), the data is stored on hardware and is processed by means of IT-systems, located on the territory of the Russian Federation.

   All the raw data, including Personal data, collected out of the Russian Federation, is localized in the regions of the use of Service in order to comply with the legislation or/and current business practices and its regulations. For data storage the Company uses physical infrastructure, situated in the regions of the use of Service.

   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.

VIII. UPDATES TO THE PRESENT POLICY

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.