JUICY LABS LIMITED LIABILITY COMPANY

RULES OF DIGITAL INTERACTION

Moscow, 2025

TABLE OF CONTENTS

TERMS, DEFINITIONS, ABBREVIATIONS

Term, abbreviation	Definition
Authentication	The process aimed at probabilistically determining a print (digital identifier or fingerprint) of the Virtual User's Device and/or Virtual User through data analysis and comparison of data on the Virtual User's Device with a diverse set of attributes and signs, without using Direct Identifiers and without enabling the Virtual User Identification.
Agreement	A confidentiality agreement and/or relevant agreement for purchasing the Software Products (license agreement or services contract) that has been agreed upon and signed by authorised representatives of both parties.
Applicable Law	A set of regulatory provisions that are effective and applicable in the Russian Federation.
Back-end Libraries	Software packages that developers use for working with server-side components of web applications.
Bonjour Protocol	A protocol for automatically discovering services on a local network.
Company	Juicy Labs Limited Liability Company (abbreviated as Juicy Labs LLC)
Contact Form	A form on the Website designed for sending contact details and messages to the Company for further interaction between the parties.
Cookie	A small piece of data made up of letters and numbers that is stored locally on the Device.
Device	A mobile or stationary device capable of connecting to the Internet, used by the Virtual User when accessing the Web Resource.
Device Fingerprinting	A technology based on unique combinations of attributes. The attributes include equipment specifications, software configuration, operating system data, browser settings, and other features, such as screen resolution, plugins, and installed fonts.
Device_ID	An anonymous identifier composed of numbers and letters. The identifier does not contain any personal information (name, email, address, etc.). It can be accessed by any application installed on the device. Unlike a device's serial number (e.g., IMEI), which is assigned by the manufacturer, the Device ID is generated by software and may change after a factory reset or application reinstallation.
Direct Identifier	A unique data attribute associated with an individual and enabling a precise match between the attribute and that individual.
Do not Track	An HTTP header that indicates whether the Virtual User requests that websites or mobile applications refrain from tracking or monitoring their actions.
Front-end libraries	Collections of functions, sub-programmes, and objects specific to a certain programming language, which are used in front-end development.
Identification	The processing of an individual's Personal Data for identifying attributes which, taken separately and/or collectively, enable unique identification of this individual.

IndexedDB	A data storage mechanism on the Virtual User's end only, which allows significant amounts of structured data to be stored, even when the web browser is closed or the system encounters a failure.
Information	Details of Virtual Users collected through software modules of the Company's Software Product in the form of a Modified Value, which do not include any Personal Data or Direct Identifiers.
JavaScript	A software based on the relevant programming language embedded in the Service for collecting the Information via the Web Resource.
KeyChain	A dedicated encrypted database for storing data (logins, passwords, authentication tokens, cryptographic keys, and other confidential data) in macOS and iOS operating systems.
Modified Value	Adding a dynamic variable set of letters, characters, and hashing to the initial value until the values are processed as part of the Software Product loop.
Natural Definiteness	The non-zero probability of randomly guessing an individual's identity.
Non-recoverable Value	A value derived from the irreversible deletion of part of the initial information, followed by hashing the remaining portion before analytical processing to prevent recovery of the initial value.
Personal Data	Any information that is directly or indirectly related to an identified or identifiable individual.
SDK	Software based on the relevant programming language embedded in the Service for collecting the Information from iOS Devices and Android Family Devices via the Web Service, as well as via the JS App – Device Risk Analytics mobile application.
Session (or JuicySession)	Information collected and retained by the Company during the period of interaction between the Software Product and the Web Resource.
Software Product (or Service)	A combination of infrastructure elements, server equipment, and software of the Company that enables the assessment of fraud risk or other operational risks based on formalised actions of Virtual Users.
Software Products Buyer	A purchaser of the Company's Software Products who has entered into the relevant Agreement with the Company.
UserAgent	A line in an HTTP request header that identifies the browsers, applications, or operating systems connecting to the server. It may include the name and version of the client application, the operating system version, device model, and language.
Virtual User	A user of the Web Resource of the Software Products Buyer in whose relation the Information is collected on the Web Resource.
Web Resource	A website, mobile application, or any other resource of the Software Products Buyer that the Virtual User can access via the Internet.
Web Session	A period of the Virtual User's interaction with the Web Resource, during which the Web Resource can "remember" certain information on the Virtual User. A session begins when the Virtual User accesses the Web Resource and ends

	when the Virtual User leaves the Web Resource or remains idle for an extended period.
Website	The Company's website accessible on the Internet at https://juicyscore.online/ the rights to which belong to the Company and which is used for posting data on the Company's products and services for information and other purposes
Zero Configuration Networking Protocol	A collection of technologies that enable automatic IP networking without requiring configuration or special servers. This protocol allows devices to automatically set up and discover each other on a network without manual intervention or a central server.

Terms or abbreviations not defined in the *Rules of Digital Interaction* shall be interpreted and used in accordance with the applicable law.

1. GENERAL

1.1. *The Rules of Digital Interaction (hereinafter referred to as the Rules)* describe the way the Company interacts with the Information obtained during the operation of the Software Products, the terms of use of the Information, and the technologies applied on the Company's Website.

1.2. *The Rules of Digital Interaction* supersede the JuicyScore Data Policy as amended on 27 April 2024 concerning interaction with the Information (previously referred to as the User Data) specified in Clause 6.3 of the *General Licensing Terms* (as amended on 22 January 2025). However, please be aware that since May 2025, the Company has been using a separate document governing Personal Data processing: the Personal Data Processing and Protection Policy, which is published on the Company's Website.

1.3. The Software Products of the Company shall be provided under the terms of separate Agreements.

1.4. The operation of the Software Products involves only the collection and sharing of the Information specified in the *Rules*. No other personal data shall be collected or shared by the Software Products.

1.5. The Company implements all necessary legal, organisational, and technical measures to protect the collected Information from unauthorised, illegal, or accidental access, destruction, modification, blocking, duplication, sharing, dissemination, and other unlawful actions concerning the Information.

1.6. The *Rules* apply to the use of the Company's software products released within the last six (6) months for front-end libraries / data collection and testing libraries, and thirty-six (36) months for back-end / scoring libraries. The Company continuously informs the Software Products Buyers about the need to make updates. The Company provides all required materials and assistance, including automatic update mechanisms for front-end libraries.

1.7. The Company reserves the right to update the *Rules* at any time at its own discretion, including but not limited to, changes related to applicable law or modifications in the operation of the Company's Software Products.

1.8. New versions of the *Rules* are published on the Website and take effect immediately upon publication. You can review the current version of the *Rules* at any time on the website: https://juicyscore.online/.

1.9. These *Rules* will be effective from 12.08.2025.

2. TYPES OF COLLECTED AND PROCESSED INFORMATION

2.1. In order to assess the risks of fraud or other operational risks that could lead to financial, reputational, or other losses for the Software Products Buyer, the Software Products are designed to collect and process the following Information via JavaScript (for web applications, in individual cases – for mobile applications), SDK (for a native mobile application)[1]:

2.1.1. General data related to the Software Products Buyer and their network resources *(JavaScript and SDK)*

2.1.2. Statistics on Virtual User activity on the Web Resource *(e. g., time spent on the Web Resource, number of corrections made while completing forms on the Web Resource) (JavaScript and SDK)*

2.1.3. Conditions and circumstances under which formalised actions are taken on the Software Products Buyer's Web Resource *(JavaScript and SDK)*

2.1.4. Data on the technical specifications of the Device *(e. g., Device make and model, screen size, memory capacity, etc.) (JavaScript and SDK)*

2.1.5. Data on the Device's basic software (*e. g., type and version of the operating system, type and version of the browser) (JavaScript and SDK)*

[1] Information is collected as part of the services provided by the Software Products Buyer to the Virtual Users via online Internet channel, subject to specific features of online to offline solutions (JS App – Device Risk Analytics and mobile SDK JuicyScore mobile application).

2.1.6. Data on the Internet connection used by the Device when accessing the Web Resource *(e. g., category of IP address, Internet bandwidth) (JavaScript and SDK)*
2.1.7. UserAgent data and other fields from the web session header *(JavaScript and SDK)*
2.1.8. Statistics on history length and URL, previous page where JavaScript is installed on the Device *(JavaScript and SDK)*
2.1.9. Statistics on categories of mobile Device applications *(via SDK only)*
2.1.10. Statistics on graphics files of the mobile Device *(via SDK only)*
2.1.11. Statistics on the utilisation level of the Device's physical resources *(JavaScript and SDK)*
2.1.12. Data associated with the geographic location of the Virtual User, approximated to within one thousand (1,000) metres *(via SDK only)*
2.1.13. Modified MAC address of a Wi-Fi router *(collection and processing of the parameter are disabled by default)*[2] *(JavaScript and SDK)*
2.1.14. Data entry rhythm *(collection and processing of the parameter are disabled by default)* [3] *(JavaScript and SDK)*
2.1.15. Data on alternative technologies *(e. g. IndexedD)*[4] *(JavaScript and SDK)*.
2.1.16. Modified value of Device_ID *(via SDK only)*.
2.1.17. Statistical and binary parameters of parallel activity on the Device during an online session *(JavaScript and SDK)*
2.1.18. Application identifier and a selective list of installed applications *(via SDK only)*
2.1.19. Information on the Device memory, with preliminary rounding of data *(via SDK only)*
2.1.20. Information on SIM card *(excluding the phone number and SIM card serial number) (via SDK only)*
2.1.21. Host name *(via SDK only)*
2.1.22. Information on the Wi-Fi connection *(via SDK only)*
2.1.23. Information on the Internet connection *(via SDK only)*
2.1.24. Information on Bluetooth[5], subject to permission only and in the form of hashed values *(via SDK only)*
2.1.25. Information on the battery *(via SDK only)*
2.1.26. Information on the mobile service provider *(via SDK only)*
2.1.27. Information on the amount of transmitted data *(via SDK only)*
2.1.28. The modified portion of the Bonjour protocol configuration data (Zero Configuration Networking protocol – "zero configuration networking") *(via SDK only)*
2.1.29. Information on the use of KeyChain *(via SDK only).*

3. TERMS OF INFORMATION COLLECTION AND PROCESSING

3.1. If the classification of the Information adopted by the Software Products Buyer categorises the Information collected by the Software Products as Personal Data, the Software Products Buyer has the option to disable any of the Information types specified in Clause 2.1 of the *Rules*.

---

[2] The collection and processing of this parameter can be activated at the discretion of the Software Products Buyer under the Agreements, provided that such actions do not infringe upon the rights and freedoms of the Virtual User and that the processing of this parameter is not classified as the processing of Personal Data.
[3] This parameter can be enabled at the option of the Software Products Buyer given the purposes of data processing if the data is required for the operation of the Web Resource, unless processing of this parameter violates the rights and freedoms of the Virtual User or is recognised as the processing of personal data as defined by applicable laws.
[4] If the Software Products Buyer needs to exclude this functionality, the Software Products Buyer shall follow the instructions given in the Company's technical documentation.
[5] By default, only data indicating whether Bluetooth is enabled or disabled will be collected; collection of other data is disabled.

3.2. The Information is collected via the Web Resources in the form of Modified Values from the Virtual User's Device strictly subject to the availability of the executed Agreement.
3.3. The processing of the Information complies with the security principles for online operation of the Virtual User and Apple and Google standards for mobile application development.
3.4. The Company does not process the Information for the purpose of Identification of the Virtual Users and has no intention of doing so in the future for minimising the risk of infringing the rights and freedoms of the Virtual Users while enhancing the value of the Information processing as an alternative to processing the Personal Data.
3.5. The Software Products Buyer shall have access to the Information only through a request via secure channels using the account that the Company has provided to the Software Products Buyer under the Agreement.
3.6. Information is transferred exclusively by submitting a request from the Software Products Buyer's infrastructure to the Company's infrastructure, following the specified technical interaction format.
3.7. A response to the request is given in the form of a response from the API Service to the extent and on the terms of the Agreement.
3.8. The response format includes, but is not limited to, the Information collected from the Software Products Buyer's Web Resources and statistics regarding the Virtual User's visits to the Software Products Buyer's Web Resources. This process does not involve explicit transmission of input data.
3.9. The Company does not provide for and prohibits any transfer of data to the Software Products Buyer outside the framework established by Agreements.
3.10. If the Company detects any Information processing of which involves individual and/or collective infringement of the Virtual Users' rights and freedoms and/or constitutes the Personal Data processing under the Applicable Law, the processing of the Information shall cease, and the relevant Information shall be destroyed.
3.11. The Software Products Buyer shall be solely responsible for the use or non-use of the Information transferred under the Agreements, and the Company shall not be responsible for any of these processes.
3.12. The Information SHALL NOT be used for active targeted marketing or customer acquisition aimed at promoting services and products of the Software Products Buyer. The use of the Software Products deliverables in violation of the aforementioned restrictions is inadmissible and prohibited, since it breaches the provisions of the *Rules* and the terms of the Agreement and may constitute a violation of the Applicable Law.
3.13. The Company DOES not process the Information that allows the Virtual User to be identified.
3.14. If the Software Products Buyer operates in a jurisdiction outside the Russian Federation, it is strongly recommended that the compliance of the Software Products and the collected Information with the laws applicable in the Software Products Buyer's jurisdiction be verified.
3.15. If the Applicable Law and/or the classification of data and/or related risks adopted by the Software Products Buyer categorise all received Information as personal data, the Software Products Buyer shall verify whether all necessary consents from personal data subjects are available, whether data processing is safe and compliant with other mandatory requirements (technical details regarding cloud data processing can be provided upon request).
3.16. If the Software Products Buyer perceives a risk associated with any specific Information / parameters collected during the operation of the Software Products and cannot disable the collection / processing of such parameters, the Software Products Buyer shall submit a request to the Company's Customer Service to set up the appropriate options (the Company will seek to accommodate such requests under the Agreements).
3.17. If the Software Products Buyer independently conducts a technical evaluation of the risks associated with processing certain types of parameters (data types), it is important to note that the more verifications are conducted, the more validated the evaluation will be.
3.18. If the Software Products Buyer identifies a risk that is many-fold higher than the existing level of the Natural Definiteness as a result of one of such verifications, it is necessary to immediately provide the

Company with a reproducible approach demonstrating that risk, and the Company will take prompt measures to eliminate the risk upon confirmation.

3.19. Please pay careful attention to how the Information is used in terms of sensitivity or potential classification of these parameters as Personal Data:

– Base data regarding Internet connections is consistently present across all sessions for all companies operating in the online environment as an integral part of any Internet connection.

– Modified MAC address of the Device – data collection is no longer performed *(this was previously done via SDK only)*. This parameter is absent for all integrations using the SDK version released by the Company after September 2023. For the SDK versions released prior to late September 2023, the collection and processing of this parameter is disabled by default, the Company no longer supports these SDK versions. It is recommended that the Software Products Buyers update their integrations to more recent versions. The processing of this parameter cannot be enabled at the discretion of the Software Products Buyer.

– Alternative technologies in the form of IndexedDB, despite the fact that sections Document.Cookie, LocalStorage, and SessionStorage incompletely coincide with Cookie, data from IndexedDB is NOT accessible to third parties and normally does not have a clear bijection between the file(s) name and the web session value. The IndexedDB value is taken from the value of one of online web sessions for hedging the risk of inadvertently capturing unauthorised data *(for hedging the risk of occurrence of values other than a random set of numbers, letters, characters, and time of the online session creation)* in the IndexedDB value.

3.20. If the processing of the Information performed for the sole purpose of identifying the risks of fraud and other operational risks, without acquiring additional Information and allowing for direct Identification of the Virtual User, but rather associating with probabilistic Authentication of the Virtual User or the Device, is treated as processing of personal data in the legal jurisdiction of the Software Products Buyer, then the Software Products Buyer shall comply with legal requirements related to personal data in their legal jurisdiction when dealing with such Information and when using the Software Products.

3.21. JuicySessions shall not be stored on the Virtual User's Device but only in the memory of the browser of the Virtual User's Device browser.

3.22. A JuicySession is generated when the Virtual User accesses the Software Products Buyer's Web Resource on the Company's servers, based on a random number generator and the timestamp of the Company's infrastructure call and therefore cannot serve as the Direct Identifiers of the Virtual User.

3.23. The JuicySession identifier depends on the random number generator and the service call timestamp and is essentially similar to a random improved token which is generated for online payments, independent of the Virtual User or their Device.

3.24. JuicySessions are not synchronised with third-party sessions. Data on the Virtual Users shall not be enriched with third-party data, including data on the Virtual Users' behaviour on other Internet resources outside of the Company's Software Products.

3.25. Considering the purposes of automated collection of the Information, the Do Not Track flag value is ignored in the operation of JuicySession and the data collection software modules operating on the Web Resource.

4. INFORMING VIRTUAL USERS

4.1. In accordance with the Applicable Law regarding the Personal Data and within the framework of recommended data management practices, the Software Products Buyer must inform the Virtual Users of its Web Resources about JuicySessions based on these Web Resources, generated by the Company, and the automated collection of the Information using the software modules provided by the Company.

4.2. The Virtual User shall be informed before any collection of the Information begins.

4.3. To assist the Software Products Buyers in fulfilling the obligation to notify the Virtual Users, the Company shall include a clause regarding Virtual User notifications in the Agreement.

4.4. The Company recommends that the following format be used for notifying the Virtual Users who visit the Web Resources:

"At the Web Resource titled *'Name of the Web Resource of the Software Products Buyer'*, for assessing the risks of claims against the product of *'Name of the Software Products Buyer'*, acting on behalf of the *'Name of the Software Products Buyer',* Juicy Labs Limited Liability Company (PSRN 1157746624826, TIN 7717294300), registered at 15A Leninsky Prospekt, intra-city area Donskoy Municipal District, Moscow, 119071, contact phone number +7 495 532-39-99, e-mail privacy@juicyscore.com, collects and processes, including storage, systematisation, accumulation, analysis, updating, retrieval, deletion and destruction, of the Information (*collected using software modules, software product of Juicy Labs LLC, technical details in the form of a modified value free of personal data*) (via JavaScript (for web applications) and SDK (for a native mobile application). The list of the Information, as well as the composition, procedure for storage and deletion is described in the *Rules of Digital Interaction* posted at https://juicyscore.online/."

5. DELETION OF INFORMATION

5.1. Since the Information collected and processed within the Company's infrastructure **is not categorised as Personal Data**, the deletion of the Information upon requests from the Virtual Users is only hypothetically possible because it is not feasible to clearly link the technical data collected by the Company to the Personal Data of the Virtual Users on the side of the Software Products Buyers.

5.2. A mechanism for submitting a request for the Information deletion is available:

– via the Contact Form on the Company's Website https://juicyscore.online/ru/ready-to-connect;

– Via a written request sent to: 15A Leninsky Prospekt, Moscow, 119071, Russia.

5.3. The deletion of the Personal Data processed by the Company is performed in accordance with the Personal Data Processing and Protection Policy.

5.4. The Company undertakes to make every effort to fulfil incoming requests for deleting the Information. Inquiries shall be considered within thirty (30) calendar days from the date of submission.

6. TECHNOLOGIES USED BY THE COMPANY AT THE WEBSITE

6.1. The Website **does not use Cookies**, meaning the files stored in the relevant section – Document.Cookies, LocalStorage, or SessionStorage in the browser database. The Company uses alternative technologies, such as persistent sessions in IndexedDB, Device Fingerprinting, and ETags.

6.2. The Website (in the Contact Form) uses various technologies, such as scripts for collecting and storing data on the Website visitors while they are present on the Website: IP address, location (country or city), type and version of the operating system on the Device, type and version of the browser on the Device, type of the Device and its display resolution, traffic source, language of the operating system and the browser, etc.

6.3. Types of technologies used on the Website:

– IndexedDB, storage period – persistently. This method of using persistent sessions on the Contact Form is designed to allow for data deletion upon request.

– Device Fingerprinting, storage period – 6 months. The Device Fingerprinting mechanism on the Contact Form is designed to allow for data deletion upon request.

7. STORAGE OF INFORMATION

7.1. The Information collected from the Web Resource for assessing the risk of the Virtual User for which the Software Products Buyer **DID NOT** make a Software Product request shall be stored for no more than thirty (30) days from the date of collection.

7.2. The Information collected from the Web Resource for assessing the risk of the Virtual User for which the Software Products Buyer made a Software Product request shall be stored for no more than two (2) years from the date of collection.
7.3. All the Information on the Virtual Users located in the Russian Federation (determined based on the Virtual User's IP address location) shall be stored on the equipment and processed using IT systems physically located in the Russian Federation.
7.4. All the initial Information collected outside the Russian Federation (determined based on the Virtual User's IP address location) is located in the regions where Software Products are used for ensuring the compliance with the law and/or existing business practices of markets and market regulations of the relevant region. The Company uses physical infrastructure located in regions where the Software Products are used for storing the Information. By default, data localisation is based on the proximity of the Virtual User's IP address to the Company's physical infrastructure used for data storage, unless other localisation is forced by the Software Products Buyer.
7.5. The Company hereby specifies that it is not the owner of the Information collected through the Software Product and processed within its IT systems. The Company ensures the secure storage of the Information under the Agreement with the Software Products Buyer.

CONTACT INFORMATION

Full business name: Juicy Labs Limited Liability Company.
Abbreviated business name: Juicy Labs LLC.
Registered address: 15A Leninsky Prospekt, Moscow, 119071.
TIN (Taxpayer Identification Number) / TRRC (Tax Registration Reason Code): 7717294300 / 772501001. PSRN (Primary State Registration Number) 1157746624826

Phone: +7 495 532-39-99

Addresses for inquiries:

- For written inquiries: 15A Leninsky Prospekt, Moscow, 119071
- E-mail: privacy@juicyscore.com