PRIVACY POLICY.

The Russian Federation, the City of Moscow.
The Tenth of December, two thousand and twenty.

This Policy in compliance with part 2 of Article 18.1 of the Federal Law of 27 July 2006 No. 152-FZ "On Personal Data" and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) specifies the policy of the Limited Liability Company “Business Club Stratton” ("the Operator") concerning the personal data processing and contains information on current Operator's requirements for the personal data protection. This Policy applies to all personal data processed through the Service that the Operator receives or may receive from the User. This Policy is an integral part of the Operator's internal document that defines the Operator's general policy regarding the processing of personal data and discloses general information about the requirements for the personal data protection implemented by the Operator.

1. GENERAL PROVISIONS.

1.1. For this Policy purposes, the below-mentioned terms and definitions mean:

"Personal data" – any information relating to an identified or identifiable natural person ("personal data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, an individual taxpayer identification number, a social security number, bank details, year, month, date and place of birth, address, email address, a telephone number, family, social, property status, education, occupation, income, metadata that are transmitted to the Operator during the Service use applying the software installed on the User's device (including location data, the HTTP headers, an IP address, "cookies", information about the User's browser, the technical specifications of the User's hardware and software, the date and time of access to the Service, the addresses of requested pages of the Service and similar information), one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For this Policy purposes, personal data also include information about the User, the processing of which is provided for in the Agreement governing the Service use. Under the Russian Presidential Executive Order of 8 March 1997 No. 188, personal data are confidential information. The Operator collects only such personal data that are necessary for the Agreement's performance.

"**GDPR**" – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Operator", "Controller" – the Limited Liability Company “Business Club Stratton” (BKS LLC), formation date: 8 April 2020, Delaware State File Number: 7928241, HBS Record ID Number: 421287, Ein 38-4151423, that processes personal data as well as determines the purposes and scope of personal data processing, and actions (operations) to be performed with personal data. The Operator is a Controller within the meaning of GDPR. Registered agent information: HARVARD BUSINESS SERVICES, INC. Address: 16192 Coastal Highway, city: Lewes, county: Sussex, State: Delaware, postal code: 19958, phone: 302-645-7400.

"Representative of the Controller" - office of the Controller on the European Union territory (EU), located at: _____ Amsterdam, the Netherlands, e-mail: amsterdam@stratton.club, designated to act instead of the Controller, in particular, in interaction with the EU supervisory authorities (independent public authorities of the EU) or the personal data subjects in the EU, on all issues related to the processing of personal data, in order to ensure compliance with the GDPR.

"User" - any fully capable individual (personal data subject), including acting on behalf of and in the interests of a legal entity, who can provide the Operator with their personal data in using the Service, who has expressed consent to the terms set out in the Agreement by signing it, including electronically, independently or as a legal entity's representative. In this Policy, a User is also a person whose personal data are processed by the Operator on behalf of the User contained in the Agreement.

"Service", "Personal Data Filing (Information) System" – under the name of the International Business Club "STRATTON CLUB", software for business owners, entrepreneurs and initiators of start-up projects, public figures, top managers of large companies that is a system of on-line services for communication, experience exchange, making transactions and obtaining resources for business on favourable terms, access to which the Operator temporarily provides the User at https://stratton.club/. Designed to work on smartphones, tablets and other User devices, mobile platforms. Includes an on-line communication platform, a mobile application, and a website https://stratton.club/, databases, program codes, know-how, algorithms, design elements, fonts, logos, as well as text, graphic and other materials, information, texts, graphic elements, images, photos, audio and video materials and other results of intellectual activity. The exclusive rights to the Service and any of its components belong to the Operator as the right-holder or licensee on the basis of a law, contract or other transaction.

"Agreement" - a license agreement/contract, transaction, user agreement or other agreement between the User and the Operator that regulates the use of the Service and contains the User's instruction to the Operator to process personal data.

"Personal data processing" - any action (operation) with personal data, including collection, recording, arrangement, accumulation, storage, specification (updating, changing), extraction, use, distribution (dissemination, provision, granting access to), anonymization, blocking, destruction of personal data.

"Processor" - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

"Recipient" - a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether or not a third party. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

"Third party" - a natural or legal person, public authority, agency or body other than the personal data subject, the Controller, processor and persons who, under the direct authority of the Controller or processor, are authorised to process personal data.

"Automated personal data processing" - personal data processing by means of computer technology.

"Non-automated personal data processing", "Personal data processing without using automation tools" – the processing of personal data in the personal data filing system or extracted from such a system in case that such actions as the use, specification, dissemination, destruction of personal data concerning each of the personal data subjects are performed with the direct participation of a natural person.

"Dissemination of personal data" – actions aimed at disclosing personal data to an indefinite range of persons.

"Provision of personal data" – actions related to making the data available to a definite person or a definite range of persons.

"Blocking of personal data" – the temporary cessation of personal data processing (except for the cases when the processing is needed for personal data specification).

"Destruction of personal data" – actions performed on personal data contained in the personal data filing system that prevent such data from being restored and (or) actions aimed at the physical destruction of the tangible medium of personal data.

"Anonymization of personal data" – actions performed on personal data that do not permit the identity of the individual concerned to be verified solely from such anonymized data. It is a "pseudonymisation", within the meaning of the GDPR.

"Use of personal data" – actions (operations) with personal data performed to make decisions, transactions or other actions that generate legal consequences for the personal data subjects or otherwise affect their rights and freedoms or the rights and freedoms of others.

"Publicly available personal data" - personal data that an unlimited number of persons have access to under the consent of the personal data subject or that, in accordance with federal laws, are not subject to the requirement of confidentiality.

"Confidentiality of personal data" - a mandatory requirement for a person who has received access to personal data to prevent their dissemination without the consent of their subject or other legal grounds.

"Statistics" - information about the Service use, as well as about the viewing by the Users of the certain Service's elements (web pages, frames, content, etc.), collected using the Counters, cookies, web beacons and other similar technologies.

"Cookies" – a small piece of data sent by the web server and stored on the User's device. Cookies contain small pieces of text and are used to store information about how browsers work. They allow to store and receive identification information and other information on computers, smartphones, phones and other devices. The RFC 2109 and RFC 2965 describe cookie specifications. For the same purposes, other technologies are used, including data stored by browsers or devices, device-related identifiers, and other software. In this Policy, all such technologies are referred to as "cookies".

"Web beacons" – images in electronic form (single-pixel (1x1) or empty GIF images). Web beacons can help the Operator in recognising certain types of information on the User's device, such as cookies, the time and date of viewing the page, and the description of the page where the web beacon is placed.

"Counter" - a part of the Service, a computer program that uses a piece of code that is responsible for analysing cookies, collecting statistical and personal data of the Users. Personal data are collected in an anonymized form.

"IP address" – a number from the numbering resource of the data transmission network built based on the protocol IP (RFC 791), which uniquely determines when providing telematics communication services, including access to the internet, the subscriber's terminal (computer, smartphone, tablet, another device) or means of communication included in the information system and owned by the User.

"HTTP header" - a string in an HTTP message that contains a colon-separated name-value pair. The HTTP header format corresponds to the general ARPA text network message header format described in the RFC 822.

"Token" - a unique set of characters that identifies the User in the accounts of third-party services. The token allows making an authorised connection to the Service using authorisation through third-party services (for example, Microsoft Authenticator, Google Authorization, social networks, Google Play, Apple AppStore, and others).

1.2. All other terms and definitions found in this Policy the Parties shall interpret under the legislation of the Russian Federation, the current recommendations (RFC) of international standardisation bodies on the Internet and the usual rules of interpretation of the relevant terms established on the Internet.

1.3. In this Policy, the terms and definitions can be used as singular or plural depending on the context, their spelling can be used with both uppercase and lowercase.

1.4. The titles of the headings (articles), as well as the design of the Policy, are intended solely for the convenience of using the text of the Policy and have no literal legal meaning.

1.5. This Policy is developed in accordance with the Constitution of the Russian Federation, the Civil Code of the Russian Federation, Federal Law of 27 July 2006 No. 149-FZ "On Information, Information Technologies, and Information Protection", Federal Law of 27 July 2006 No. 152-FZ "On Personal Data", and other federal laws. For the Users in the European Union, it also considers the mandatory requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (*GDPR*).

1.6. This Policy defines the procedure and conditions for the personal data processing by the Operator, including the order of transfer of personal data to third parties, peculiarities of non-automated personal data processing, the order of access to personal data, the personal data security, organisation of internal control and liability for violations of personal data processing, and other issues.

1.7. This Policy comes into effect from the moment of its approval by the Operator and is valid indefinitely until it is replaced by a new policy.

1.8. The Operator has the right to change this Policy without the User's consent. All changes to the Policy are made by the Operator's administrative act.

1.9. This Policy applies to all personal data processing processes carried out using the Service without the use of automation tools. The Operator does not control and is not responsible for the services owned by third parties, to which the User can click on the links posted in the Service.

2. LEGAL GROUNDS FOR PERSONAL DATA PROCESSING.

2.1. The Operator processes the User's personal data in accordance with the following documents:

- Constitution of the Russian Federation;
- Civil Code of the Russian Federation;
- Tax Code of the Russian Federation;
- Federal Law of 27 July 2006 No. 152-FZ "On Personal Data»;
- Federal Law of 27 July 2006 No. 149-FZ "On Information, Information Technologies, and Information Protection";
- The Law of the Russian Federation of 7 February 1992 No. 2300-1 "On Consumer Rights Protection»;
- Resolution of the Government of the Russian Federation of 15 August 1997 No. 1025 "On Approval of the Rules of Consumer Services in the Russian Federation»;
- The Decision of Goskomstat of the Russian Federation of 5 January 2004 No. 1 "On Approval of the Unified Forms of Primary Records for Labor Accounting and Remuneration»;
- Resolution of the Government of the Russian Federation of 15 September 2008 No. 687 "On Approval of the Regulation on the Specifics of Personal Data Processing Carried Out Without the Use of Automation Tools»;
- Resolution of the Government of the Russian Federation of 1 November 2012 No. 1119 "On Approval of Requirements for the Personal Data Protection During Their Processing in Personal Data Information Systems»;
- Order of the FSTEC (ФСТЭК) of Russia of 18 February 2013 No. 21 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Personal Data Security During Their Processing in Personal Data Information Systems»;
- Order of the Federal Security Service of Russia (ФСБ России) of 10 July 2014 No. 378 "On Approval of the Composition and Content of Organisational and Technical Measures to Ensure the Personal Data Security When Processing Them in Personal Data Information Systems Using Cryptographic Information Protection Tools Necessary to Meet the Requirements for Personal Data Protection Established by the Government of the Russian Federation for Each of the Security Levels»;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR);
- other regulatory legal acts in the relevant field of activity of the Operator.

2.2. The processing of the User's personal data is carried out on the basis of and in compliance with the Agreement governing the use of the Service, and other transactions, agreements or contracts concluded between the User and the Operator, or on the basis of the User's separate consent to such processing.

3. THE PURPOSES OF PERSONAL DATA COLLECTION.

3.1. The Operator processes only those personal data that are necessary for the Service use or the execution of transactions, agreements and contracts with the User, unless the law of the Russian Federation or the European Union provides for mandatory storage of personal information for a period specified by law.

3.2. When processing personal data, the Operator does not combine databases containing personal data, the processing of which is carried out for incompatible purposes.

3.3. The Operator processes the User's personal data for the following purposes:

3.3.1. use of personal data of the Users who are natural persons utilising the Service on their own behalf to conclude and execute an Agreement or any other transaction with the Operator;

3.3.2. use of personal data of the Users who are natural persons utilising the Service on behalf of a natural or legal person represented by them to conclude and execute an Agreement or any other transaction with the Operator;

3.3.3. conducting statistical and other studies of the Service use based on anonymized data;

3.3.4. compliance with the mandatory requirements of the legislation of the Russian Federation or the European Union.

4. THE SCOPE AND CATEGORIES OF PERSONAL DATA PROCESSED,

THE CATEGORIES OF PERSONAL DATA SUBJECTS.

4.1. The Operator processes personal data necessary for the execution of an Agreement, or other transaction with the User.

4.2. Personal data allowed for processing under this Policy and provided by the Users-individuals who utilise the Service on their own behalf, by filling in the input fields when using the Service, may include the following information:

4.2.1. last name, first name, patronymic (if any);

4.2.2. the address of the personal data subject, the number of his principal identification document and information as to the date of issue of that document and the body which issued it;

4.2.3. year, month, the date of birth;

4.2.4. location;

4.2.5. workplace, the type of economic activity carried out;

4.2.6. education;

4.2.7. photo;

4.2.8. video image;

4.2.9. the audio recording of the voice;

4.2.10. e-mail address;

4.2.11. mobile phone number;

4.2.12. the password to log in to the Service;

4.2.13. the data of social networks through which the User enters the Service;

4.2.14. token;

4.2.15. the HTTP headers;

4.2.16. the IP address of device;

4.2.17. cookies;

4.2.18. data collected by the Counters;

4.2.19. data got using the Web beacons;

4.2.20. information about the browser;

4.2.21. the technical specifications of the device and software;

4.2.22. technical data about the Service operation, including the dates and time of use and access to it;

4.2.23. the addresses of the requested Service pages;

4.2.24. geolocation data.

4.3. Personal data allowed for processing under this Policy and provided by the Users-individuals utilising the Service on behalf of a natural or legal person represented by them, by filling in the input fields when using the Service, may include the following information:

4.3.1. last name, first name, patronymic (if any);

4.3.2. the address of the representative of the personal data subject, the number of his principal identification document, information as to the date of issue of that document and the body which issued it and details of the power of attorney or another document confirming the representative's authority;

4.3.3. year, month, the date of birth;

4.3.4. location;

4.3.5. workplace, the type of economic activity carried out;

4.3.6. education;

4.3.7. photo;

4.3.8. video image;

4.3.9. the audio recording of the voice;

4.3.10. e-mail address;

4.3.11. mobile phone number;

4.3.12. the password to log in to the Service;

4.3.13. the data of social networks through which the User enters the Service;

4.3.14. token;

4.3.15. the HTTP headers;
4.3.16. the IP address of device;
4.3.17. cookies;
4.3.18. data collected by the Counters;
4.3.19. data got using the Web beacons;
4.3.20. information about the browser;
4.3.21. the technical specifications of the device and software;
4.3.22. technical data about the Service operation, including the dates and time of use and access to it;
4.3.23. the addresses of the requested Service pages;
4.3.24. geolocation data.
4.4. Personal data processed in accordance with this policy and automatically transmitted to the Operator during the use of the Service using the software installed on the User's device may include the following information:
4.4.1. the HTTP headers;
4.4.2. the IP address of device;
4.4.3. cookies;
4.4.4. data collected by the Counters;
4.4.5. data got using the Web beacons;
4.4.6. information about the browser;
4.4.7. the technical specifications of the device and software;
4.4.8. technical data about the Service operation, including the dates and time of use and access to the Service;
4.4.9. the addresses of the requested Service pages;
4.4.10. geolocation data.
4.5. Under this Policy, the Operator processes personal data of persons belonging to the following categories of personal data subjects:
4.5.1. natural persons who use the Service in accordance with the Agreement on its use on their own behalf;
4.5.2. natural persons who use the Service in accordance with the Agreement on its Use on behalf of the natural or legal person represented by them.

5. PROCEDURE AND CONDITIONS FOR PERSONAL DATA PROCESSING.

5.1. The Operator has the right to process the User's personal data without notifying the authorized body for the protection of data subjects under part 2 of Article 22 (clauses 2 and 8) of the Federal Law "On Personal Data".
5.2. The Operator processes the User's personal data using the personal data information system without using automation tools in accordance with the regulatory legal acts of the Russian Federation that establish requirements for ensuring the security of personal data during their processing and for observing the rights of personal data subjects. Such actions with personal data, as the use, specification, dissemination, destruction of personal data in relation to the User, are carried out with the direct participation of the Operator's employees in accordance with the peculiarities approved by the Decree of the Government of the Russian Federation of 15 September 2008 No. 687.
5.3. The Operator processes and stores the User's personal data within the period determined under the Agreement on the Service use, or within such a period that the Operator reported to the User when getting the User consent to the processing of personal data by other means (in check-box, SMS, email, etc.).
5.4. With respect to the User's personal data, their confidentiality is maintained, except in cases of voluntary provision by the User of information about himself for general access to an unlimited number of persons.
5.5. The Operator has the right to distribute the User's personal data to the Processor, Recipient, or Third parties in the following cases:
5.5.1. the User requested the Operator for such a transfer;
5.5.2. there is a User's consent to such actions;
5.5.3. the distribution is necessary for the User to utilise certain functionality of the Service (for example, for authorisation through social media accounts) or for the execution of a certain agreement, contract or transaction with the User;

5.5.4. the distribution is provided for by the legislation of the Russian Federation or other legal norms within the framework of the procedure established by regulatory legal acts;

5.5.5. in case of transfer of rights to the Service, it is necessary to transfer personal data to the acquirer simultaneously with transferring all obligations to comply with the terms of this Policy in relation to the personal data received by him;

5.5.6. to ensure the protection of the rights and legitimate interests of the Operator or third parties when the User violates this Policy or the Agreement on the Use of the Service;

5.5.7. in other cases, provided for by regulatory legal acts.

5.6. The Processors can be:

- the website hosting provider;
- the operator of an electronic platform for the mobile application distribution;
- other persons who will be entrusted with the processing of personal data on behalf of the Operator.

5.7. In relation to the User in the EU, in the case of his/her personal data breach, the Operator shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent EU Supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

5.8. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Operator shall communicate the personal data breach to the User without undue delay. The communication to the data subject shall not be required if any of the following conditions are met: (a) the Operator has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the Operator has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; (c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

5.9. The Operator takes the necessary organisational and technical measures to protect the User's personal data from unauthorised or accidental access, destruction, modification, blocking, copying, distribution, as well as from other illegal actions of third parties.

5.10. The Operator, together with the User, takes all necessary measures to prevent losses or other negative consequences caused by the loss or unauthorised disclosure of the User's personal data.

5.11. The Operator has the right to distribute personal data to the bodies of inquiry and investigation, other authorised bodies on the grounds provided for by regulatory legal acts.

5.12. When collecting personal data, the Operator records, arranges, accumulates, stores, specifies (updates, changes), and extracts personal data of the Users who are citizens of the Russian Federation using databases located on the territory of the Russian Federation.

5.13. The Operator ceases processing the User's personal data, which processing is carried out with the User's consent, at the expiration of the User's consent to the processing, or when the User withdraws the consent to the personal data processing, and in case the unlawful personal data processing is detected, or the Operator's liquidation.

6. ACCESS TO PERSONAL DATA.

6.1. Right of access to the User's personal data to the only employees of the Operator and/or Processor is given in the virtue of duty to work with personal data of the User under the list of persons allowed to work with personal data, which is approved by the Operator and/or the Processor.

6.2. The Operator and/or the Processor keeps up-to-date the list of employees who have received access to personal data.

6.3. Without the User's consent, access to the User's personal data by persons who are not employees of the Operator and/or the Processor is prohibited, except in cases established by regulatory legal acts.

6.4. The access of the employee of the Operator and/or the Processor to the personal data of the User is terminated from the date of employment termination or the date of loss by the employee of the right of access to the

User's personal data because of the change in duties, position or other circumstances under the Operator/the Processor's order. In the event of the employment relationship termination, all media containing the User's personal data that were at the disposal of the dismissed employee of the Operator/the Processor is transferred to a higher-ranking employee in the order established by the Operator/the Processor.

7. THE UPDATING, CORRECTING, DELETING AND DESTROYING OF PERSONAL DATA.

7.1. At any time, the User can change, update, supplement or delete the personal data provided by him/her or part of them using the Service interface.
7.2. If the Operator independently identifies the fact of incompleteness or inaccuracy of the User's personal data, the Operator takes all possible measures to update the personal data and make appropriate corrections.
7.3. If it is impossible to update incomplete or inaccurate personal data of the User, the Operator takes measures to delete them.
7.4. In case of detection of the illegality of the User's personal data processing, the Operator ceases their processing, and the personal data are subject to deletion.
7.5. If the Service interface is inoperable or the Service is not functional enough to change, update, supplement or delete personal data by the User, and in any other cases, the User has the right to demand in writing from the Operator to specify his/her personal data, block or destroy them because the personal data are incomplete, outdated, inaccurate, illegally obtained or unnecessary for the stated purpose of processing.
7.6. The Operator changes the personal data that are incomplete, inaccurate or outdated within a period not exceeding seven working days from the date when the User provided with information confirming that the personal data are incomplete, inaccurate or outdated.
7.7. The Operator shall destroy the User's personal data that are illegally obtained or are unnecessary for the stated purpose of processing within a period not exceeding seven working days from the date of submission by the User of information confirming that such personal data are illegally obtained or are unnecessary for the stated purpose of processing.
7.8. The Operator notifies the User of the changes made and the measures taken and takes reasonable measures to notify the persons to whom the personal data of this User has been transferred.
7.9. The User's rights to change, update, supplement or delete personal data may be restricted under the requirements of regulatory legal acts. Such restrictions, in particular, may provide for the Operator's obligation to preserve the personal data changed, updated, supplemented or deleted by the User for a period determined by regulatory legal acts and to transfer such personal data to state authorities following the established procedure.

8. RESPONSES TO THE USER REQUESTS FOR ACCESS TO PERSONAL DATA.

8.1. The User has the right to receive information from the Operator concerning the processing of his personal data, including information containing:
8.1.1. confirmation of the processing of personal data by the Operator;
8.1.2. legal grounds and purposes of personal data processing;
8.1.3. methods of personal data processing used by the Operator;
8.1.4. name and location of the Operator, information about persons (except for employees of the Operator) who have access to personal data or to whom personal data may be disclosed on the basis of a contract with the Operator or regulatory legal acts;
8.1.5. processed personal data related to the User, the source of their receipt, unless a different procedure for submitting such data is provided for by a regulatory legal act;
8.1.6. terms of processing of personal data, including the terms of their storage;
8.1.7. procedure for the User to exercise the rights provided for in the regulatory legal acts in the field of personal data;
8.1.8. information on the cross-border transfer of data that has taken place or is expected to take place;

8.1.9. the name or last name, first name, patronymic and address of the person performing the processing of personal data on behalf of the Operator, if the processing is or will be entrusted to such a person;

8.1.10. other information provided by regulatory legal acts.

8.2. The Operator provides free of charge the opportunity to get acquainted with the personal data processed and stored in the Operator's information system when the User applies within thirty calendar days from receipt of the User's written request.

8.3. If the Operator refuses to provide information about the availability of personal data about the User or personal data to the User upon receipt of the User's request, the Operator shall reasoningly respond in writing, which is the basis for such refusal, within a period not exceeding thirty calendar days from receipt of the User's request.

9. INFORMATION ABOUT THE IMPLEMENTED REQUIREMENTS FOR THE PERSONAL DATA PROTECTION.

9.1. The security of personal data during their processing in the personal data information system is ensured by a personal data protection system that neutralises current threats identified under part 5 of Article 19 of the Federal Law "On Personal Data".

9.2. The Operator applies a personal data protection system that includes legal, organisational, technical and other measures to ensure the security of personal data, determined considering current threats to the security of personal data and information technologies used in information systems.

9.3. Regarding personal data in respect of which the User has granted consent to their processing by the Processor, the Operator has the right to engage, on the basis of the contract, a Processor who ensures the security of such personal data when processing them in the information system.

9.4. The Operator, when processing personal data in its information system, provides:

9.4.1. implementation of measures aimed at preventing unauthorised access to the User's personal data and/or transfer of them to persons who do not have the right to access such information;

9.4.2. timely detection of unauthorised access to personal data;

9.4.3. prevention of impact on the technical means involved in the processing of personal data, as a result of which their functioning may be disrupted;

9.4.4. possibility of immediate recovery of personal data modified or destroyed due to unauthorised access to them;

9.4.5. constant control over ensuring the level of personal data protection.

9.5. In order to comply with security requirements and implement a personal data security system, the Operator has developed a private security threat model for the personal data information system.

9.6. The Operator under the Resolution of the Government of the Russian Federation of 1 November 2012 No. 1119 "On Approval of Requirements for the Personal Data Protection During Their Processing in Personal Data Information Systems" defined the level of protection of personal data during their processing in personal data information system owned by the Operator.

9.7. The Operator has drawn up an act to determine the level of protection of personal data during their processing in the personal data information system.

9.8. The Operator, based on the act of determining the level of protection of personal data during their processing in the personal data information system without the use of automation tools, has developed and implemented a set of measures to protect and ensure the security of personal data.

9.9. The Operator uses technical means and software for the processing and protection of personal data, as well as keeps a log of personal data protection tools.

9.10. The Operator keeps a log of accounting and storage of removable media containing personal data.

9.11. Technical means that ensure the functioning of the personal data information system are placed in premises owned by the Operator on the right of ownership or another property right (rent, gratuitous use, etc.).

9.12. All employees working with personal data, as well as associated with the operation and maintenance of the information systems of personal data, are familiar with the requirements of this Policy and internal documents of the Operator governing the handling of personal data.

9.13. The Operator has organised training for employees on the use of personal data protection tools operated by the Operator. Training is provided to employees who have permanent access to personal data, and employees

associated with the operation and maintenance of the personal data information system and personal data protection tools.

9.14. The Operator's internal documents establish that employees must inform immediately the relevant official of the Operator about the loss, damage or shortage of information carriers containing personal data, and about the attempts of unauthorised access to personal data, its causes and conditions.

10. CONSENT TO THE PERSONAL DATA PROCESSING.

10.1. The User decides to provide his / her personal data and consents to their processing freely, at his / her own will and in his / her own interest.

10.2. The consent to the processing of personal data provided by the User is freely given, specific, informed and unambiguous.

10.3. In the case of processing the User's personal data on the basis of and in compliance with the Agreement governing the Service use and other transactions, agreements or contracts concluded between the User and the Operator using the Service, such processing of the User's personal data is carried out on the basis of clause 5 of part 1 of Article 6 of the Federal Law "On Personal Data", point (b) of Article 6(1) of the GDPR and does not require separate consent.

10.4. In the case of the processing of personal data of the User based on his explicit consent to such processing, expressed directly in the Service use by pressing the corresponding button, by putting a mark indicator corresponding check-box, sending text messages, or e-mail, such consent to the personal data processing is provided by the User as an electronic document signed by a simple electronic signature under the Agreement governing the Service use.

10.5. The User can revoke the consent to the personal data processing under the procedure established by regulatory legal acts.

11. FINAL PROVISIONS.

11.1. The beginning of the Service use by the User means that the User agrees to the terms of this Policy. If the User does not agree with the terms of this Policy, the use of the Service must be terminated immediately.

11.2. The law of the Russian Federation shall apply to this Policy and to the relations between the User and the Operator arising in connection with the application of this Policy. The Users located in the European Union are also subject to the GDPR.

11.3. This Policy is permanently publicly available at the following link: https://stratton.club/en/documents/privacy-policy.pdf.

11.4. The User has the right to send all suggestions or questions about this Policy to the Operator's User Support service by emailing the following email address: support@stratton.club; e-mail address for the Users in the European Union: amsterdam@stratton.club.

12. BANK DETAILS.

The Limited Liability Company “Business Club Stratton” (BKS LLC), formation date: 8 April 2020, Delaware State File Number: 7928241, HBS Record ID Number: 421287, Ein 38-4151423, registered agent information: HARVARD BUSINESS SERVICES, INC. Address: 16192 Coastal Highway, city: Lewes, county: Sussex, State: Delaware, postal code: 19958, phone: 302-645-7400