Privacy Policy for the Hotel Booking Platform "Moya Bron"

1. General Provisions

- This Privacy Policy (hereinafter referred to as the "Policy") has been developed by Moya Bron LLC (OGRN 1247700470566, INN 9717165404, legal address: 129626, Moscow, Mira Avenue, building 102, block 1, premises 3/7) (hereinafter referred to as the "Operator") in accordance with the requirements of the legislation of the Russian Federation, including Federal Law No. 152-FZ of July 27, 2006 "On Personal Data," and defines the procedure for processing and protecting the personal data of users of the hotel booking service carried out through the Telegram messenger (hereinafter referred to as the "Platform"). The Operator guarantees compliance with the rights of personal data subjects and takes necessary measures to ensure the security of personal data.
- The Policy applies to any information about users that the Operator may obtain when using the Platform. Personal data (hereinafter referred to as "PD") means any information relating directly or indirectly to a specific or identifiable individual (User). This Policy is an integral part of the user agreement (offer agreement) for the use of the Platform. The User's commencement of Platform use or provision of their personal data means consent to this Policy and confirmation that the User has provided their PD voluntarily.
- The processing of Users' personal data is carried out by the Operator – Moya Bron LLC. The Operator independently or with the involvement of third parties organizes the processing of PD and determines the purposes of processing, the composition of collected PD, and actions (operations) performed with PD. The Operator's contact details are provided in Section 9 of this Policy.
- The Operator collects, records, stores, and destroys personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation, in accordance with the requirements of the current legislation of the Russian Federation. The Operator is guided by the provisions of Federal Law No. 152-FZ "On Personal Data" and other regulatory legal acts of the Russian Federation in the field of personal data protection.

2. Personal Data Collected by the Platform

The Operator collects and processes the following personal data of Users necessary for providing hotel booking services:

- **User's surname and name.** For booking a hotel in the User's name.
- **Phone number.** For contacting the User regarding booking confirmation, providing order status notifications, and support service communication.
- **Email address.** For sending booking confirmations, payment receipts, informational letters related to service provision, and document exchange.
- **Booking data.** Information about the selected hotel (hotel name), check-in/check-out dates (booking date), room type, and accommodation cost. This information is necessary for arranging and fulfilling bookings and generating reporting documents.
- **Payment data.** For accommodation payment, payment card data or other details necessary for processing payment through an integrated payment system (CloudPayments) may be requested. Attention: payment card data is entered by the User on a secure CloudPayments payment page; the Operator does not directly store or process the full card number and other sensitive payment data – their processing is performed by a third-party payment service (see Section 5).
- **Communication data.** Content of User inquiries to the support service (via Telegram chat) and other information that the User voluntarily provides when communicating with the Operator. This data may include additional contact or identifying information if the User decides to communicate it during the inquiry.
- **Technical and analytical information.** When using the Platform, some technical data is automatically collected: User device IP address, device type used, operating system version, browser information (if applicable), language, approximate geographic location, data about the facts and time of Platform function use. Collection of this information is carried out using cookies and similar technologies by analytical systems (such as Yandex.Metrica and Google Analytics) to improve service operation, usage statistics, and ensure information security (for more details on data transfer to analytics systems, see Section 5).

The Operator does not request or process special categories of personal data (about racial or ethnic origin, political views, religious or philosophical beliefs, health status, intimate life) or biometric personal data within the Platform's operation. Users are required to provide accurate and current data; the consequences of providing inaccurate information are borne by the User in accordance with the User Agreement.

3. Purposes of Personal Data Processing

Users' personal data is collected and processed by the Operator strictly for specific, predetermined, and lawful purposes. The main purposes of PD processing on the Platform include:

- **Providing booking services.** Arranging and ensuring hotel booking at the User's request. Surname, name, and booking data (hotel, dates, room type) are used to reserve a room in the

User's name through a partner booking system.

- **Contract fulfillment and feedback.** Contacting the User via provided phone number or email to transmit booking confirmation, voucher, information about changes or order status, and to send payment reminders if necessary. Contact data is used to fulfill obligations to the User within the framework of the booking service provision agreement.

- **Payment processing.** Organizing payment acceptance for booked accommodation. User payment data is used to conduct transactions through the integrated payment service (CloudPayments). The purpose of processing is to accept payment and ensure fulfillment of financial obligations (invoicing, payment confirmation).

- **User support.** Processing User inquiries and requests through the Telegram support service chat. Personal data contained in such inquiries (such as Telegram username, inquiry content, contact details) is used exclusively for User consultation, resolving arising issues, correcting possible booking problems, and improving service quality.

- **Service improvement and analytics.** Analyzing User activity on the Platform to improve service operation, develop new functions, and enhance interface convenience. For this purpose, the Operator uses technical and behavioral analytics data (such as function usage statistics, traffic, typical bot interaction paths). Anonymized data may be used for statistical and research purposes to identify service usage trends. Web analytics tools (Yandex.Metrica, Google Analytics) help the Operator obtain aggregated statistics and understand audience needs; the Operator strives to anonymize or aggregate data for analytical reports when possible.

- **Ensuring security.** Processing technical data and log files to ensure Platform information security, prevent fraud, unauthorized access, and other unlawful actions. For example, IP addresses and other technical information may be used to detect suspicious activity, protect against DDoS attacks and other threats, and investigate information security incidents.

- **Compliance with legal requirements.** The Operator's compliance with mandatory requirements of Russian Federation legislation, for example, in the field of accounting, tax reporting, storage of accounting documents, and execution of lawful requests from government authorities. Personal data may be used for generating and storing documents (contracts, invoices, acts) for periods established by legislation, as well as for providing information to authorized government bodies in cases provided by law (such as by court or law enforcement request).

The Operator does not process personal data for purposes incompatible with those initially stated. If it becomes necessary to use data for a new purpose different from those specified above, the Operator will request preliminary User consent for such processing, except in cases expressly permitted by legislation.

4. Legal Grounds for Processing

The Operator processes Users' personal data on the following lawful grounds provided by the legislation of the Russian Federation on personal data:

- **User consent.** PD processing is carried out with the consent of the personal data subject – the User (in accordance with clause 1, part 1, Article 6 of Federal Law No. 152-FZ). The User provides the Operator with consent to process their personal data by performing implied actions – continuing to use the Platform, arranging bookings, transmitting their data through the Platform interface, marking consent to Policy terms, etc. Consent is valid until its withdrawal by the User (see Section 6 on User rights to withdraw consent).

- **Contract performance.** PD processing is necessary for the performance of a contract to which the User is a party or beneficiary (clause 5, part 1, Article 6 of Federal Law No. 152-FZ). This means that personal data is processed to provide the User with hotel booking services, fulfill related settlement and other obligations. For example, without processing contact and identification data, the Operator cannot confirm and fulfill the booking, and without processing payment data – accept payment.

- **Other grounds.** In certain cases, the Operator may process personal data without User consent if such processing is permitted by legislation. Such cases include, in particular: the necessity to fulfill the Operator's obligations established by law (clause 2, part 1, Article 6 of Law 152-FZ), the necessity to protect life, health, or other vital interests of the User or other persons in cases where obtaining consent is difficult (clause 6, part 1, Article 6), the necessity to exercise rights and legitimate interests of the Operator or third parties, provided that the rights and freedoms of the PD subject are not violated (clause 7, part 1, Article 6). The Operator also has the right to process personal data made publicly available by the User themselves (clause 10, part 1, Article 6). The listed cases usually occur when processing is dictated by legal requirement or extraordinary circumstances.

In all situations where separate consent of the PD subject is required according to legislation (for example, when transferring data to countries that do not ensure adequate PD protection, when publicly distributing PD, etc.), the Operator requests such consent from the User in the required form. The Operator strictly complies with the principles and conditions of personal data processing provided by law.

5. Transfer of Personal Data to Third Parties

The Operator does not disclose or transfer Users' personal data to third parties, except in cases listed below, or when such transfer is provided by legislation or expressly permitted by the User. Data transfer to third parties is carried out in the volume necessary to achieve the specified processing purposes, while complying with confidentiality and security requirements. The main recipients (third parties) to whom User data may be transferred include:

- **CloudPayments payment service.** To process booking payment, the Operator interacts with the external CloudPayments payment system. As part of payment, the User may be redirected to a secure CloudPayments gateway where they enter their bank card data. The CloudPayments service receives such information as cardholder name, card number, expiration date, security code, and payment amount, and may also receive contact details (such as phone or email for sending payment notification). Transfer of this data is necessary for authorization and processing of payment transactions. CloudPayments acts as an independent operator (processor) of payment data and processes it according to its own privacy policy. The Operator transfers to CloudPayments minimally necessary information (such as order identifier, amount payable, currency, payer name) and does not receive access to full bank card details (except card type and part of the number). All interaction with CloudPayments is protected by encryption means complying with payment card industry security standards (PCI DSS).

- **"Bronevik" booking system (Bronevik API).** The Platform is integrated with the external Bronevik hotel booking service to obtain current hotel information and make bookings. To confirm the User's selected accommodation option, the Operator transfers necessary personal data through a secure channel to the Bronevik system: guest (User) surname and name for hotel booking registration, as well as booking details (hotel name, stay dates, selected rate/room type). This data is used by the partner (Bronevik) exclusively for booking arrangement and information transfer to the respective hotel facility. Bronevik acts as a partner personal data operator and ensures confidentiality of received information according to its agreement with the Operator and legal requirements. Without transferring this data, booking a room in the User's name would be impossible.

- **Analytics services (Yandex.Metrica and Google Analytics).** For collecting statistics and improving Platform operation, the Operator uses web analytics services Yandex.Metrica (provided by Yandex, Russia) and Google Analytics (provided by Google LLC, USA). These services, using cookies and similar technologies, obtain and process anonymized data about User activity: visited pages or bot commands, number of bookings made, technical information about device and browser, approximate location (country/city by IP), etc. Yandex.Metrica provides the Operator with reports in aggregated form that do not reveal the specific User's identity. Google Analytics also collects analytical data; some data may be transferred and processed on servers outside the Russian Federation (for example, in Google data centers in other countries). The Operator has concluded necessary agreements with these services and/or configured them to ensure confidentiality compliance (in the case of Google Analytics, the Operator may use the IP address anonymization feature). Data collected by analytical systems is not used to establish User identity but serves to understand general activity and audience preferences. Users may, if desired, disable cookie storage in their browser settings, but this may affect the correct operation of some Platform functions.

- **Telegram messenger (support service).** User support inquiries are processed via chat in the Telegram messenger. This means that User messages containing personal data (such as Telegram profile name, inquiry text, possible attachments) pass through Telegram infrastructure. Telegram

may act as an independent operator of correspondence data and store message history in accordance with its privacy policy. The Operator does not transfer to Telegram any additional User data beyond what the User communicates in the chat. Correspondence with the User is used by the Operator only to respond to inquiries and resolve User problems. Caution is recommended when transmitting confidential information through the support chat. The Operator is not responsible for data security on the Telegram messenger side; Users should familiarize themselves independently with Telegram's data processing terms. At the same time, Operator support service employees undertake to maintain correspondence confidentiality with the User and not disclose information obtained during communication to third parties without lawful grounds.

- **Government authorities and other third parties by law.** The Operator has the right to provide personal data to authorized government authorities (such as inquiry and investigation bodies, courts, tax authorities, Roskomnadzor) in cases and procedures established by the legislation of the Russian Federation. Such transfers are carried out only in the presence of a lawful request and strictly in the volume required in accordance with law. Additionally, within the framework of legal requirements, the Operator may transfer data for accounting and tax reporting (for example, payment information – to banking or tax institutions if provided by regulations). In all cases of data provision based on law, the Operator preliminarily verifies the request's lawfulness and ensures transfer through secure communication channels.

The Operator guarantees that under no circumstances does it sell or provide Users' personal data to third parties for commercial purposes not specified in the Policy without direct User consent. Transfer of PD to third-party organizations not named in this Policy is possible only on the basis of separate explicit User consent or direct legal prescription. All third-party organizations involved in personal data processing are bound by obligations to protect the confidentiality of received information and use Users' personal data only for those purposes that were provided to them by the Operator.

6. User Rights (Personal Data Subject Rights)

The Operator respects the rights of each User as a personal data subject and ensures the possibility of their implementation in accordance with Chapter 3 of Federal Law No. 152-FZ. A User whose data is processed on the Platform has the following rights:

- **Right to information about processing of their PD.** Users have the right to receive from the Operator confirmation of the fact of processing their personal data, as well as information about purposes, legal grounds, processing methods, processing (storage) periods of their PD, the name and location of the Operator, the presence of data relating to this User at the Operator, and the composition of such data. Upon request, Users are provided with information about persons who have access to their PD or to whom data may be disclosed based on an agreement with the Operator or in accordance with law. The procedure for requesting such information is indicated below (in this section and in Section 9).

- **Right to access their personal data.** Upon User request, the Operator provides copies or otherwise familiarizes the User with their personal data being processed, except in cases provided by law (for example, if data contains information about another subject or state secret). Provision of information is carried out within a reasonable time and, as a rule, free of charge (if the request is not repetitive or excessive, as established by law). Users may request this information by sending a corresponding request to the Operator in writing or in electronic document form signed with an electronic signature (in accordance with Russian Federation legislation).

- **Right to clarification, blocking, or destruction of PD.** If Users discover that their personal data is incomplete, outdated, inaccurate, or was obtained illegally or is not necessary for the stated processing purpose, they have the right to demand from the Operator: (a) clarification (updating, correction) of their data; (b) blocking of data (temporary suspension of processing) – for example, if the User disputes data correctness or processing lawfulness, for the verification period; (c) destruction of personal data if processing was carried out in violation of legal requirements or if data is no longer required to achieve stated purposes. Users may send such requirement to the Operator in free form (via email or postal address specified in Section 9). The Operator undertakes to review such requirement and provide a reasoned response within the timeframes established by law (no more than 10 working days for data correction or destruction from the moment of receiving the request or consent withdrawal, if there are no other lawful grounds for processing).

- **Right to withdraw consent.** In cases where personal data processing is carried out based on User consent, the PD subject has the right to withdraw their consent at any time by sending a corresponding notification to the Operator. Consent withdrawal does not have retroactive effect and means that further processing of data that was carried out exclusively based on consent will be terminated by the Operator. Upon receiving consent withdrawal for PD processing, the Operator undertakes to cease processing and (if PD storage is no longer required for processing purposes or by law) destroy personal data within a period not exceeding 30 days, or ensure their destruction (if processing is performed by another person on behalf of the Operator). It is important to note that in case of consent withdrawal for processing data necessary for service provision (for example, contact details for arranging a current booking), the Operator may be unable to continue providing corresponding services to the User.

- **Right to object to processing or restrict processing.** In cases provided by law, Users have the right to object to the Operator's processing of their personal data if they consider that such processing affects their rights and legitimate interests. In particular, PD subjects have the right at any time to object to processing of their personal data for direct marketing purposes (distribution of advertising or promotional materials); upon receiving such objection, the Operator will immediately cease processing the User's PD for marketing purposes. Users may also demand to restrict (temporarily suspend) processing when disputing data accuracy or processing lawfulness.

- **Right to protect their rights and appeal.** If Users believe that the Operator violates personal data legislation requirements or infringes on their rights and freedoms, they have the right to file a complaint directly with the Operator (for prompt problem resolution) or submit an appeal to the

authorized supervisory authority – the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). Users also have the right to judicial protection of their rights. Roskomnadzor contact details and complaint filing procedure are available on the agency's official website. The Operator recommends first addressing any questions or complaints regarding PD processing directly to the Operator – this will allow resolving the situation most quickly and efficiently.

To exercise their rights, personal data subjects may send the Operator a written or electronic request formatted in accordance with legislative requirements. The request should indicate the User's full name, the essence of the inquiry, and contact details for communication. The Operator undertakes to review the inquiry and provide a response or requested information within no more than 30 days from the date of inquiry receipt (unless another period is established by legislation). In case of refusal to satisfy the User's request (partially or completely), the Operator will provide a reasoned response indicating the grounds for refusal.

7. Personal Data Protection Measures

The Operator takes necessary legal, organizational, and technical measures to protect Users' personal data from unlawful or accidental access, destruction, modification, blocking, copying, distribution, as well as from other unlawful actions. In accordance with the requirements of Article 19 of Federal Law No. 152-FZ, internal data security documents have been developed and applied, and modern protection means have been implemented. The main measures implemented by the Operator to ensure PD confidentiality and security include:

- **Data storage in a protected environment.** Users' personal data is stored in databases on servers located in the Russian Federation, which complies with the personal data localization requirement (Federal Law No. 242-FZ). Servers are located in data centers with restricted access equipped with security control and monitoring systems (24-hour security, video surveillance, access control system).

- **Encryption and data transmission.** Encryption is used when collecting and transmitting confidential data. All information that the User provides through the Platform interface (including personal data entry and payment) is transmitted through secure communication channels (SSL/TLS protocol). Payment operations through CloudPayments are carried out on encrypted pages using high-level encryption protocols. This prevents interception and unauthorized access to data during transmission over the Internet.

- **Access restriction and rights differentiation.** Only those Operator employees or associated persons who need it to perform their duties and provide services have access to Users' personal data ("need to know" principle). Each such employee acts on the basis of the Operator's instructions and undertakes to maintain confidentiality of processed data (corresponding non-disclosure agreements are signed). Information systems implement access rights differentiation:

accounts and rights are configured so that employees see only data related to their area of competence.

- **Passwords and authentication.** Complex passwords and multi-factor authentication mechanisms (if applicable) are used to access databases and administrative panels. Passwords are periodically changed in accordance with security policy. Access to critical system nodes is possible only from trusted IP addresses or through secure VPN connections.

- **Antivirus protection and updates.** Current antivirus software is installed on servers and workstations involved in PD processing; scanning for malicious code is regularly performed. Software and hardware are promptly updated to current versions to eliminate known vulnerabilities and increase overall infrastructure security.

- **Backup and recovery.** The Operator performs backup of key databases and systems in case of failure or information loss. Backup copies are stored in encrypted form. Data recovery procedures from backup copies are regularly tested, allowing prompt system operation resumption in case of emergency and minimizing data loss risk.

- **Monitoring and audit.** The Operator monitors information security events: access logs to personal data and key actions with them are maintained. These logs are regularly reviewed for suspicious activity. Additionally, internal checks of Policy and legislation compliance are periodically conducted (internal audit). When necessary, the Operator involves external specialists for security assessment (penetration testing, security audit).

- **Personnel training.** Operator employees authorized to process personal data undergo appropriate training and instruction on personal data handling rules and security measures. The Operator ensures that employees are familiarized with the provisions of Russian Federation legislation on personal data, local acts on PD protection, and establishes disciplinary liability for violations in this area.

- **Incident response.** In case of detection of unauthorized access or personal data leakage, the Operator immediately conducts an investigation, notifies authorities when necessary (including Roskomnadzor if the incident falls under the criteria established by Russian Federation Government Decree), and takes measures to eliminate violation consequences. Users whose data may have been affected by the incident will be notified if required by law or if the Operator deems it necessary to protect their rights.

Personal data in the Operator's information systems is protected in accordance with requirements established for the corresponding security level (FSTEC Russia Order No. 21, FSB Russia Order No. 378, etc.). The Operator continuously improves the data protection system as technologies develop and new security methods appear.

8. Personal Data Retention Periods

The Operator processes and stores Users' personal data no longer than required by the processing purposes specified in this Policy and mandatory legislative requirements. PD retention periods are established considering the following principles:

- **Duration of service provision.** Basic personal data (name, contacts, booking data) is stored throughout the entire period of service provision to the User (until booking completion, trip, or other service provision) and for a reasonable period after its completion to ensure the possibility of claim resolution, refunds, warranty provision, etc. Usually, specific booking data is stored until hotel check-out and additionally for 5 years after service provision (in accordance with statute of limitations periods and financial reporting requirements).

- **Legislative storage requirements.** The Operator is obliged to store certain information for a certain period by law. For example, accounting documents containing personal data (invoices, acts, payment information) must be stored for at least 5 years after the end of the reporting year, and contracts with Users – for 4 years (the general statute of limitations period for civil claims). In such cases, PD will be stored for the period prescribed by corresponding legislation.

- **Storage until consent withdrawal/purpose fulfillment.** Personal data processed based on User consent (for example, data for newsletter distribution if such distribution is conducted) is stored until consent withdrawal, unless a shorter period is established during data collection. Personal data no longer necessary for processing purposes is subject to deletion or anonymization. Upon achieving processing purposes (for example, after service provision and expiration of storage periods required by law), all User-related personal data is either destroyed within the timeframes established by internal regulations or anonymized, i.e., deprived of characteristics allowing user identification.

- **Deletion upon request.** Upon reasoned User request to cease processing and/or destroy personal data (for example, if the User has withdrawn consent or considers processing illegitimate), the Operator reviews the inquiry and, if there are grounds, ceases processing and deletes corresponding data (if their storage is not required by law). The fact of personal data destruction is documented by a destruction act. Some information may be retained in backup copies until their cyclical deletion, but it will not be used in operational activities after the deletion decision is made.

Upon expiration of the above storage periods, the Operator either destroys personal data or anonymizes it, excluding the possibility of User identification. Anonymous aggregated data (not allowing establishment of User identity) may be stored without time limitation, as it does not constitute personal data.

9. Personal Data Operator Contact Details

The operator of Platform Users' personal data is Moya Bron LLC. Users may send any requests, questions, or comments related to their personal data and this Policy to the following contact details:

- **Operator's location address:** 129626, Russian Federation, Moscow, Mira Avenue, building 102, block 1, premises 3/7.
- **Email address:** support@moyabron.ru (for personal data subject inquiries).
- **Telegram support service:** @moyabronsupport_bot (weekdays from 9:00 to 18:00, Moscow time).

The Operator recommends contacting by email or Telegram for prompt review of personal data processing issues. The inquiry should briefly state the essence of the request and, if possible, indicate full name and contact phone number for feedback. Upon receiving an inquiry, the Operator will register it and provide a response within the timeframe established by legislation (see Section 6).

If the User requires an official written response (for presentation to other organizations, etc.), they have the right to send a request by registered mail to the Operator's postal address specified above or present it in person at the Operator's location during reception hours. Such request must indicate full name, identity document details, essence of requirement, and applicant's signature.

10. Final Provisions

- **Policy validity.** This Policy comes into force from the moment of its approval by the Operator and is valid indefinitely until replaced by a new version. The current version of the Policy is available to Users in open access – the Operator posts the Policy text on the official website (if available) or provides it upon request through the support service. It is recommended to periodically familiarize yourself with the current version of the Policy.
- **Changes and additions.** The Operator reserves the right to make changes to this Privacy Policy. Changes may be due to changes in legislation, Platform functionality development, changes in PD processing conditions, or introduction of new services. In case of significant changes (for example, changes in the list of collected data, purposes, or third-party transfers), the Operator will notify Users through an announcement on the Platform (or other available means, such as email distribution). The new version of the Policy comes into force from the moment of its publication (unless otherwise provided by the new version itself). Further User use of the Platform after changes come into force means User consent to the updated Policy.
- **Other documents.** Other documents regulating personal data processing and confidentiality issues (such as User Agreement, PD Processing Consent, etc.) may also be in effect in relations between the User and the Operator. In case of contradiction between the provisions of this Policy and other documents directly concerning personal data protection, the provisions of the document version published later apply.
- **Additional agreements.** If individual agreements are concluded between the Operator and the User affecting personal data processing and protection issues (such as separate written consent

or contract), the terms of such agreement have priority in the part not contradicting mandatory legal requirements.

- **Implementation control.** Responsibility for organizing storage and ensuring personal data security is borne by the person designated by the Operator as responsible for PD processing. Compliance with the requirements of this Policy is monitored by the Operator's management. Persons guilty of violating norms regulating personal data processing and protection bear responsibility in the manner established by the legislation of the Russian Federation.

This Privacy Policy is drafted in Russian. Moya Bron LLC undertakes to comply with the personal data processing principles set forth in it. By using the Platform's services, Users confirm that they are familiar with the terms of this Policy, understand them, and express their consent to personal data processing in accordance with the specified terms.