DATA PROCESSING POLICY
FOR MOBILE APPLICATION «FLEXY Booking» AND WEBSITE FLEXY.PRO

1. TERMS AND DEFINITIONS

«**Automated processing of personal data**» shall mean processing of personal data using computer technology.

«**Controller**» shall mean the person responsible for the processing and protection of the Personal Data of Users located in the EU within the meaning of the General Data Protection Regulation of April 27, 2016 (hereinafter the «**GDRP**»).

«**Website**» shall mean a set of graphic and information materials, as well as computer programs and databases, ensuring their availability on the Internet at the network address **flexy.pro**, including all subdomains.

«Mobile Application» shall mean software (with all existing additions and improvements) designed to run on smartphones, tablets, watches and other mobile devices, and developed for a specific platform (iOS, Android, HMS, etc.). For the purposes of this Policy, the Mobile Application means the following software: **FLEXY Booking**.

«**Data Processing System**» shall mean the Website and the Mobile Application together.

«**Personal data**» shall mean a set of personal data and/or non-personalized information about the User provided by the Data Controller himself and/or automatically collected by the Data Controller and/or third parties.

«**Policy**» shall mean this Data Processing Policy, with all existing additions and changes.

«**User**» shall mean a legal entity or an individual who has downloaded the Mobile Application on a smartphone, tablet, watch or any other mobile device and/or has activated (i.e. completed the process of authorization, registration and other similar actions) of such a Mobile Application on one of the specified devices, or any visitor to the Website.

«**User Agreement**» shall mean an agreement concluded between the Data Controller and the User regarding the procedure, rules and features of the User's usage of the Mobile Application. The User joins such an agreement and does not have the right to make and/or demand the introduction of any changes or additions to it.

«Processing of personal data» shall mean any action (operation) or a set of actions (operations) performed using automation tools or without using such tools with personal data, including collection, recording, systematization, accumulation, storage, clarification (update, change), extraction, use, transfer (dissemination, provision, access), depersonalization, blocking, deletion, destruction of personal data.

«Data Controller» shall mean a state body, municipal body, legal entity or individual, independently or jointly with other persons organizing and (or) carrying out the processing of personal data, as well as determining the purposes of processing of personal data, the content of personal data to be processed, actions (operations) performed with personal data. For the purposes of this Policy, the **Data Controller** or **the Company** shall mean **MSP INEX DIGITAL LTD**.

«Data Processor» shall mean a person who, in the understanding of the GDRP, on behalf of the Data Controller, stores and/or processes Personal Data received from Users.

«Provision of Personal Data» shall mean actions aimed at disclosing personal data to a certain person or a certain circle of persons.

«Dissemination of Personal Data» shall mean any actions aimed at disclosing personal data to an indefinite circle of persons (transfer of personal data) or at acquaintance with the personal data of an unlimited number of persons, including the disclosure of personal data in the media, posting in informational and telecommunication networks or providing access to personal data in any other way.

«Cross-border transfer of Personal Data» shall mean the transfer of personal data to the territory of a foreign state to the authority of a foreign state, to a foreign individual or foreign legal entity.

«Destruction of Personal Data» shall mean any actions as a result of which personal data are destroyed irrevocably with the impossibility of further restoring the content of personal data in the personal data information system and (or) the material carriers of personal data are destroyed.

«Cookies» shall mean small files sent by any mobile application or site and placed on smartphones, tablets, watches and other mobile devices of the User to improve the operation of such applications or sites, as well as the quality of the content posted therein.

2. GENERAL PROVISIONS

2.1. The Company collects, retains, and uses personal data, including biometric data, for the purpose of verifying the identity of individuals, who use or have used the Mobile Application or Face recognition (Face-ID) equipment that uses biometric identification systems to increase security and controls access. The Company recognizes the sensitivity of personal data and biometric information and takes seriously its obligations to maintain the confidentiality and protect the security of data. The Company considers face geometry and face and photo images as "Biometric Identifiers". "Biometric Data" is Biometric Identifiers that are used to identify a person.

2.2. Purpose:
In accordance with the data protection laws, including GDPR et seq., and other laws and regulations, this Policy sets forth the Company's procedures for disclosure, storage, and destruction of personal data, including biometric information.
More specifically, (i) for safety and security reasons, (ii) to verify the users of the Company's service and equipment, and (iii) in an effort to prevent and combat fraud, the Company may compare photo imagery of the users from the Company's timekeeping technology with profile imagery to confirm identities using facial recognition technology. This process involves detecting and comparing faces from the imagery through the use of biometric data, such as facial geometry.

2.3. This Policy regarding the processing of personal data (hereinafter – the «**Policy**») applies to all information that the Data Controller may receive about visitors to the **Website** and the **FLEXY Booking Mobile Application**.

2.4. User rights for the protection of personal data
In connection with the provision of Personal Data, the User automatically receives the following rights:
(1) receive data concerning their processing (the grounds and purposes of such processing, the processing methods used, information about the persons who have access to data or to whom data may be disclosed on the basis of an agreement or the Law).
(2) receive data on the location and identification data of persons who process Personal Data.
(3) receive data on the storage periods of Personal Data.
(4) receive data on the performed or expected cross-border transfer of Personal Data.
(5) receive information about the location and identification of data of persons who store Personal Data.
(6) appeal against the actions or inaction of the Data Controller to the authorized body for the protection of the rights of subjects of personal data or in court.
(7) exercise other rights in the field of personal data protection provided for by the laws or the provisions of this Policy.

3. LIST OF COLLECTED PERSONAL DATA

3.1. Non-personalized information about Users
In connection with the use of the Mobile Application and the Website, the Data Controller may automatically collect and process the following non-personalized information about the User:
(1) information about traffic, the possible number of clicks, logs and other data.
(2) information about the location of the User (geolocation). Geolocation in the Mobile Application works constantly, even when the User is not using the Mobile Application.
(3) information about the device (identification number, mobile operator's network) from which log in is performed, operating system, platform, browser type and other information about the browser, IP address, used Wi-Fi networks.

3.2. Personal data about users
The User provides the Data Controller with the following personal data:
(1) surname, name, patronymic;
(2) email address.
(3) mobile phone number.
(4) a photograph of the User.

(5) the data contained in the personal account (profile) of the User, all internal correspondence of the User within the Mobile Application, as well as other activity of the personal account (profile) of the User.
(6) payment information, including card details, other similar information (if applicable);
(7) data on purchases made by Users and/or received/paid services through the Mobile Application (if applicable);
(8) professional and employment-related information, including the name of the employing company, position, department, other information about the User's profession;
(9) information from the Email/Outlook Calendar, when using the respective integration and booking.
(10) device and usage information, including information about a computer or mobile device (device identifiers such as IP address, WiFi and Bluetooth MAC address), geolocation information (such as based on a GPS or WiFi signal of a mobile device depending on the settings of the latter).
(11) data and information obtained as a result of combining certain Personal data of a specific User, as well as data and information received data about the User received from third parties (partners, marketers, researchers);
(12) User's ID or other identifying document data (if applicable);
(13) photo and biometric data of the User.

3.3. The User is the only person responsible for the completeness of the provided personal (biometric) data and is obliged to timely change them (update, check, correct) on a regular basis.

3.4. The Data Controller assumes that all personal (personal) data provided by the User are reliable, and that the User maintains such information up to date.

3.5. Biometric data and respective Policy implementation
3.5.1. Consent
An individual's biometric data will not be collected or otherwise obtained by the Data Controller without prior consent of the individual. The consent form will inform the individual of the reason the biometric Information is being collected and the length of time the data will be stored.

3.5.2. Disclosure
The Data Controller will not disclose or disseminate any biometric data to anyone other than its biometric identifier collector vendor(s) and/or licensor(s), unless:
1. Disclosure is required by law or other ordinance,
2. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction,
3. The User has consented to such disclosure or dissemination.

3.5.3. Storage
In circumstances where the Data Controller retains biometric information, the Data Controller will use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Data Controller stores, transmits and protects from disclosure other confidential and sensitive information that is used to uniquely identify an individual.

3.5.4. Retention Schedule
In circumstances where the Data Controller retains biometric information, the Data Controller will permanently destroy an individual's biometric data within twelve (12) months of when the initial purpose for collecting or obtaining such biometric data has been satisfied and/or when the Information has not been used to identify the person for twelve (12) months. If any Data Controllers' vendors and/or licensors require access to biometric data in order to fulfill the purpose of collecting such information, the Data Controller will request that they follow the above destruction schedule.

3.6. Information about the transactions being made
The User, through the Mobile Application, can pay for goods or services by entering information about the payment card and the identification data of the owner of such a card in a special field. The user can make a payment in the Mobile application in the following ways:
• by bank card.
• using the Apple Pay payment system.
• using the Google Pay payment system.

3.6.1. The collection and processing of data about the User in this case is carried out solely for the purpose of making payment, preventing fraud, as well as complying with other requirements of the Law.

3.6.2. The User agrees to access and collection by the Data Controller and the relevant payment system or the banking institution through which the payment is made to such Personal Data, and agrees with the Data Processing policy of the relevant payment system or banking institution.

3.7. Use of Cookies

The Mobile Application and the Website use certain tracking tools Cookies to store the IP address, User preferences or the type of device used in order to:

(1) keeping statistics of website visits and traffic,

(2) personalization of the data displayed on the User's screen,

(3) storing data necessary to identify the User, including when accessing from different devices and respective preferences,

(4) displaying advertisements in accordance with the interests and preferences of the User. The mobile application can use both its own cookies belonging to the Data Controller and third-party cookies.

3.8. The Mobile Application and the Website use the following Cookies:

(1) *Technical (functional) Cookies*, which are needed to control traffic and data transfer, to identify Users and provide the User with access to the content of the Mobile Application and without which the use of the Mobile Application is functionally limited, as well as to prevent the provision of recommendations that do not correspond to the interests of the User.

(2) *Statistical Cookies*, which are needed to track the frequency of visits to the Website by Users, to identify how the User uses the Mobile Application, as well as to identify the type and kind of content that is popular with or interesting for the User.

(3) *Geolocation Cookies*, which are needed to determine the location of the User to personalize the content displayed on the screen of his device in the Mobile Application.

(4) *Cookies of third parties*, which are installed by third parties with the permission of the User and are intended to conduct statistical research regarding the behavior of the User on the Internet and/or the sending of personalized advertising or marketing materials to the User and/or the provision of goods or services.

3.9. The User has the right to disable Cookies at any time in the Mobile Application and on the Website by changing certain settings on the computer, smartphone, tablet, watch or other mobile device. Such disconnection may entail restriction or change of the User's access to the functionality of the Mobile Application and/or content.

4. PURPOSES OF COLLECTING AND PROCESSING OF PERSONAL DATA

4.1. Determination of the purposes of processing

The purpose of processing the User's personal data is the conclusion, execution and termination of civil contracts; providing the User with access to services, services, information and/or materials contained on the Website, as well as all subdomains of **flexy.pro**, and in the Mobile Application.

4.2. The collection and processing of Personal Data is carried out for the following purposes:

(1) to analyze the behavior of the User, as well as to identify the User's preferences for a certain type of content.

(2) for the prompt and correct operation of the Mobile Application, improving the functioning of the Mobile Application, improving the content of the Mobile Application, improving the internal architecture and functionality of the Website and the Mobile Application.

(3) to identify the User.

(4) to send personalized news and marketing materials to the specified email address and/or mobile phone of the User.

(5) to comply with legal and other applicable regulations.

(7) to determine the location of the User.

(8) for technical support of the Mobile Application, identifying problems in its operation and their elimination.

(9) to keep the communication with the User (communication).

(10) to fulfill other obligations of the Data Controller that arose before the User.

(11) for statistical research.

(12) to enforce contractual rights, comply with financial reporting requirements, court orders, requirements or subpoenas in accordance with applicable law.

(13) for any other purpose, subject to obtaining a separate consent from the User.

4.3. Anonymized data collected using Internet statistics services is used to collect information about the actions of Users on the site, improve the quality of the site and its content.

4.4. The processing of Personal Data is carried out on the basis of the principles of:

(1) legality of the purposes and methods of processing;

(2) good faith;
(3) compliance of the purposes of processing Personal Data with the purposes predetermined and declared in the collection of such Personal Data; and
(4) extent and nature of the processed Personal Data is consistent with the stated purposes of their processing.

4.5. Personal data processing conditions
Personal data processing is carried out in the following cases:
(1) obtaining consent from the User;
(2) achieving the goals stipulated by an international treaty or law;
(3) provision by the User of his personal data to an unlimited number of persons (via publication, Internet resources, etc);
(4) fulfillment of other obligations of the Data Controller to the User, including, but not limited to, the provision of certain content to the User; or
(5) saving the life or health of the User, when consent to the processing of his Personal data cannot be obtained in advance.

4.6. By filling out the appropriate forms and/or sending personal data to the Data Controller, the User agrees with this Policy.

4.7. The Data Controller processes anonymized data about the User if it is allowed in the settings of the User's browser (the storage of cookies and the use of JavaScript technology are enabled).

4.8. In the case of anonymization of Personal Data, which does not directly or indirectly determine the User, the subsequent use and disclosure of such data to third parties is allowed and the rules of this Policy no longer apply to them.

4.9. The Data Controller takes all possible measures to protect the confidentiality of the received Personal Data, except for cases when the User has made such data publicly available.

4.10. The processing of Personal Data is carried out using automation tools and without using such automation tools.

5. ACCESS OF THIRD PARTIES TO PERSONAL DATA

5.1. Use of analytical platforms
The Data Controller uses analytical platforms such as Google Analytics, , Sentry to **(1)** track the frequency of visits to the site by Users; and **(2)** tracking how the User uses the Mobile Application and / or its content; and **(3)** identifying the type and type of content that is popular with Users; and **(4)** determining the location of the User. The User also gives his consent to the Data Controller for his use of the information received about the User using the specified analytical platforms, and also expresses his consent to the Privacy Policies/Data Protection Policies of the analytical platforms Google Analytics, Sentry in their editions in effect at the time the Mobile Application is used by the User:

- Google Analytics Privacy Policy: https://policies.google.com/technologies/ads?hl=en; https://policies.google.com/privacy?hl=en (text and URL are subject to change at Google's discretion);
- Sentry's privacy policy: https://sentry.io/privacy/ (text and URL are subject to change at Sentry's discretion).

5.2. For these purposes, each analytical platform may collect data about the IP address, geolocation, actions of User, as well as User’s preferences and interests in relation to certain content.

5.3. Analytical platforms gain access to Personal Data in order to provide the Data Controller with an understanding of how effectively the Mobile Application works, what kind of content is popular, how effective is the placement of certain advertisements, as well as for the purposes of developing and/or improving the existing marketing strategy Data Controller.

5.4. By installing the Mobile Application and/or using the Website, the User agrees with the automatic installation of the corresponding Cookies on the User's device.

5.5. Disclosure of personal data to third parties
The Data Controller has the right to disclose Personal Data
(1) to its affiliates, branches and representative offices opened both on the territory of the Russian Federation and on the territory of other states;

(2) in order to fulfill legal obligations, including with the participation of auditors, lawyers, accountants and other consultants;
(3) as part of compliance with laws and responding to procedural notices or requests from government or law enforcement agencies;
(4) to detect, limit and prevent fraud or to confirm and enforce the policies governing the provision of the Services;
(5) the legal successors of the Data Controller who arose as a result of its liquidation, reorganization or bankruptcy, and who received exclusive rights to own the Data Processing System;
(6) to payment service providers or banking (financial) institutions, for conducting transactions of the User through the Mobile Application or the Website;
(7) to third parties solely for the purpose of obtaining or accessing certain content by the User;
(8) to third parties, when the User has given consent to the disclosure, transfer or processing of his Personal Data, as well as in other cases expressly provided for by the Law or this Policy.

5.6. The Data Controller discloses Personal Data only if **(1)** is sure that third parties will comply with the terms of this Policy and take the same measures to protect the confidentiality of Personal Data that the Data Controller takes, and **(2)** consent to such disclosure has been previously expressed User and/or allowed by law.

6. PLACEMENT OF ADVERTISING

6.1. Distribution of news and marketing materials

The User automatically, upon installing the Mobile Application on the device and registering on the Website, agrees with the Data Controller's right to send personalized news and marketing materials to the provided email address and/or mobile phone, as well as notifications related to the procedure for using the Mobile Application and the Website, and/or their content.

7. SENDING COMPLAINTS AND REQUESTS TO THE DATA CONTROLLER

7.1. Rights in relation to information: access, clarification, deletion and restriction

The User has the right to:
(i) request confirmation regarding the storage, use or transfer of any Personal Data;
(ii) gain access to Personal Data or a copy of it;
(iii) restrict usage by Data Controller of Personal Data or object to certain uses as described above;
(iv) request correction of inaccurate, incorrect or incomplete Personal Data; or
(v) request the deletion of Personal Data stored by the Data Controller, subject to certain exceptions provided by law.

7.2. Request to terminate the processing of Personal Data

Each User has the right to express objection to the Data Controller against the processing and/or storage of Personal Data. Such an objection can be expressed by sending to Data Controller to the email address: support@multispace.global.
If the User provides consent to the Data Controller for the use of biometric information, the User has the right to withdraw his consent at any time in accordance with applicable law. Upon withdrawal of such consent, the Data Controller reserves the right to refuse to provide the User with all or part of the services.

7.3. Request for information about Personal Data

If the User has questions related to the procedure for applying or using this Policy, the procedure and/or method of processing Personal Data, the User can sent such question to the email address: support@multispace.global.

7.4. Change (update, addition, correction) or deletion of personal data

The User has the right at any time to independently change or delete his Personal Data, unless such change or deletion may lead to **(1)** a violation of the rules of this Policy; or **(2)** a violation of the Law**; (3)** the nature of such Personal Data is evidence in any legal proceeding between the Data Controller and the User. To do this, the User needs to delete personal account (profile) in the Mobile Application.

7.5. The Data Controller has the right at any time to delete the User's personal account/profile, as well as all Personal Data about the User if he has violated the terms of this Policy and/or the User Agreement.

8. TERMS AND PROCEDURE OF STORAGE OF PERSONAL DATA

8.1. The Data Controller stores Personal Data as long as the legal relationship between the User and the Data Controller continues and for a certain period after their termination. Personal information that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

8.2. In determining such retention period, we take into account the time during which such Personal Information is required to:

- continue to develop, customize, modernize and improve our Services;
- maintain business records for analysis and/or audit purposes;
- comply with the requirements for the storage of documents in accordance with the law;
- protect interests in connection with any existing or potential claims; or
- respond to any complaints about the services.

8.3. Notwithstanding the above provisions of this Section , the Company will retain documents (including electronic documents) containing personal data:

(a) to the extent that we are required to do so by law;
(b) if we believe that the documents may be relevant to any ongoing or prospective legal proceedings; and
(c) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

8.4. The Data Controller ensures the safety of personal data and takes all possible measures to exclude access to personal data of unauthorized persons.

8.5. Storage can be carried out by third parties on behalf of the Data Controller. The User gives his consent to the storage of his Personal Data by third parties on behalf of the Data Controller, provided that such third parties preserve the confidentiality of the received Personal Data.

8.6. The Data Controller can carry out the functions of storing Information independently, or they can be entrusted to another person (hereinafter referred to as the «**Processor**»). Since the person storing Personal Data may be located in the territory of the European Union/European Economic Area, the User hereby gives his consent to the cross-border transfer of Personal Data and storage outside the Russian Federation.

8.7. Before starting the cross-border transfer of personal data, the Data Controller is obliged to make sure that the foreign state, to whose territory it is supposed to transfer personal data, provides reliable protection of the rights of subjects of personal data.

8.8. Cross-border transfer of Personal Data on the territory of foreign states that do not meet the above requirements can be carried out only if there is a written consent of the subject of personal data to the cross-border transfer of his Personal Data and/or the execution of an agreement to which the subject of personal data is a party.

8.9. Storage is carried out for the entire period necessary to achieve the stated purposes of processing Personal Data.

8.10. The Data Controller undertakes to destroy or depersonalize immediately after achieving the goals of processing Personal Data.

9. ACCESS OF MINORS TO THE DATA PROCESSING SYSTEM

9.1. Users in the European Union

The use of the Mobile Application is intended for persons aged 16 and over, who gain access to it only subject to prior consent to the processing of their Personal Data.

10. PROCEDURE FOR PROTECTING PERSONAL DATA

10.1. Protecting the confidentiality of Personal Data is the primary and important task for the Data Controller. The Data Controller adheres to all required international standards, rules and recommendations for the protection of Personal Data.

10.2. The Data Controller has implemented a number of reasonable appropriate technical and organizational measures aimed at protecting Personal Data from disclosure or unauthorized access to them by third parties, including from

unauthorized or illegal processing, accidental loss, destruction or damage. Despite the measures taken, the Data Controller cannot guarantee the security of any information, and the User transfers Personal Data at his own risk. The User is obliged to comply with the Data Controller's requirements in relation to security controls (using a strong password, refusing to transfer credentials to other users, logging out of the system, following other security recommendations).

10.3. To ensure the safety and confidentiality of the received Personal Data, the Data Controller uses the following protection measures:
(1) SSL (Security Sockets Layer) protocol;
(2) SET (Secure Electronic Transaction) protocol;
(3) Automatic saving of data;
(4) Firewalls;
(5) Web Application Firewall;
(6) Regular security audits of the Data Processing System.

11. USERS IN THE TERRITORY OF THE EUROPEAN UNION

11.1. General Provisions

Since the Mobile Application is available to users from the European Union, the Data Controller undertakes to additionally adhere to the provisions of the GDRP.

11.2. The controller in the understanding of this Policy is the Data Controller. The processor in the understanding of this Policy is the Processor in accordance with Article 8 of the Policy.
The Data Controller stores Personal Data for a reasonable period of time necessary to achieve the purposes of processing, but not less than the period established by the local legislation of the Member State of the European Union, on the territory of which the Mobile Application is available, for storing this or that type of Personal Data. Upon the expiration of the period established for storage, the Data Controller undertakes to immediately destroy or anonymize such data.

11.3. User rights in the field of Personal Data protection

According to Chapter 3 of the GDRP, Users located in the European Union have the following rights in the field of Personal Data protection: **(1)** the right to receive information about their Personal Data ("the right to be informed"); and **(2)** the right to access your Personal Data ("the right of access"); and **(3)** the right to rectification of Personal Data ("the right to rectification"); and **(4)** the right to erasure of Personal Data ("the right to erasure"); and **(5)** the right to restrict the processing of Personal Data ("the right to restrict processing"); and **(6)** the right to transfer Personal Data to third parties ("the right to data portability"); and **(7)** the right to object ("the right to object").

12. FINAL PROVISIONS

12.1. Availability of Policy text for review

Users can familiarize themselves with the terms of this Policy at the following link:
https://my.flexy.pro/files/public/privacy_policy.pdf
This Policy might be translated into a foreign language for those Users who access the Mobile Application and/or Website outside the Russian Federation. In case of discrepancy between the original text (Russian) and its translation, the original language shall prevail.

12.2. This version of the Policy is valid from April 11, 2022.

12.3. Changes and additions to the policy

Any information that is collected as part of the Services is governed by the Policy in effect at the time such information is collected. The Data Controller reserves the right to change, add or remove parts of this Policy at any time and at its sole discretion.

12.4. This Policy is subject to change from time to time. The Data Controller does not bear any responsibility to the User for changing the terms of this Policy without the permission and/or consent of the User.

12.5. The user himself undertakes to regularly check the provisions of this Policy for possible changes or additions. Your continued relationship with us upon posting or notifying you of any change to this Policy constitutes your agreement to be bound by the terms of any such change. Any changes to this Policy are effective at the time of publication or introduction by the Data Controller.

12.6. Applicable law

This Policy has been developed in accordance with the current legislation on the protection of personal data of the European Union, as well as the provisions of the General Data Protection Regulation dated April 27, 2016 GDRP.

12.7. Disclosure risk

Regardless of the measures taken by the Data Controller to protect the confidentiality of the personal data received, the User is hereby considered to be duly aware that any transfer of Personal Data on the Internet cannot be guaranteed safe, and therefore the User carries out such transfer at his own risk.