PERSONAL DATA PROCESSING POLICY
FOR PERSONAL DATA PROVIDED BY DATA SUBJECTS

TERMS AND DEFINITIONS USED IN THIS POLICY

– **«Personal Data»** means any information relating to an identified or identifiable natural person (data subject), including but not limited to: first name, last name, contact details, account information, payment details, identification documents, online identifiers, technical data, as well as any other information that directly or indirectly allows a person to be identified;

– **«Data Subject»** means any natural person whose Personal Data is processed by the Controller, including Website Users, clients, representatives of corporate clients and partners, persons registered in the Controller's online services, as well as persons sending requests via contact forms, messengers and other communication channels;

– **«Processing of Personal Data»** means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, systematization, structuring, accumulation, storage, clarification (updating, modification), use, analysis, transfer (provision, disclosure, dissemination or other access), restriction, blocking, deletion, destruction, anonymization, as well as cross-border transfer;

– **«Controller»** means MAIZON GROUP L.L.C-FZ, a free zone company incorporated and existing in accordance with the laws of the United Arab Emirates, which determines the purposes and means of Processing of Personal Data;

– **«Processor»** means any legal or natural person, institution or other body which Processes Personal Data on behalf of the Controller on the basis of an appropriate contract or other legal ground;

– **«Confidentiality of Personal Data»** means the obligation of the Controller, its employees, Processors and other persons having access to Personal Data not to disclose such data to third parties and not to disseminate it without a legal ground, the consent of the Data Subject or another case provided for by Applicable Law;

– **«Automated Processing of Personal Data»** means Processing of Personal Data using information systems and computing facilities;

– **«Anonymization of Personal Data»** means actions as a result of which it becomes impossible, without using additional information, to determine that Personal Data relates to a specific Data Subject;

– **«Pseudonymisation of Personal Data»** means Processing of Personal Data in such a manner that, without the use of additional separately stored information, Personal Data can no longer be attributed to a specific Data Subject;

– **«Cross-border Transfer of Personal Data»** means transfer of Personal Data to the territory of another state or to an international organisation, including storage on servers located outside the UAE or providing remote access to Personal Data from outside the UAE;

– **«Website / Site»** means the aggregate of information and other materials available on the Internet at: https://bezebee.com, as well as other domains and subdomains administered by the Controller, on which there is an explicit reference to this Policy;

– **«Controller's Programs and Online Services»** means software products, personal accounts, forms, CRM systems, online platforms, advertising accounts, integrations with external services and other tools through which the Controller provides services and/or interacts with Users;

– **«Cookies»** means small pieces of data sent by a web server and stored on the User's device (computer, smartphone, tablet, etc.), containing anonymized or personalized information about the User's actions on the Website and/or in online services, technical parameters of the device, browser settings and other data used to identify the browser/device and to configure the display of the Website and services;

– **«Applicable Law»** means the applicable laws of the United Arab Emirates, including Federal Decree-Law № 45 of 2021 on the Protection of Personal Data (UAE Personal Data Protection Law, PDPL), relevant secondary legislation, as well as other applicable regulatory legal acts of the UAE and the Emirate of Dubai, including acts of the authorities of free zones in which the Controller is registered.

1. GENERAL PROVISIONS

1.1. This Policy determines the procedure and conditions for Processing Personal Data provided by Data Subjects to the Controller in connection with the use of the Website, online services and services of the Controller, participation in marketing and other events, as well as under any forms of interaction with the Controller via the contacts indicated on the Website.

1.1.1. All issues related to Processing of Personal Data are governed by this Policy, the internal documents of the Controller, the terms of contracts concluded with Users and clients, as well as Applicable Law in the field of Personal Data protection and confidentiality.

1.1.2. This Policy also serves as a privacy policy in relation to the use of the Website and other online services of the Controller and governs the procedure for collection, use, systematization, storage and disclosure of information about Users and Clients, including their Personal Data, within the functioning of the said services of the Controller.

1.2. This Policy has been developed taking into account the requirements of Applicable Law of the UAE in the field of Personal Data protection and is intended to ensure proper protection of the rights and freedoms of Data Subjects, as well as transparency and predictability of the Controller's actions with respect to Processing of such data.

1.3. The current version of the Policy is a public document and is available on the Internet on the Website. The Controller is entitled to periodically update the Policy, including in connection with changes to the functionality of the Website, services of the Controller, its activities or Applicable Law. The new version enters into force from the moment it is published on the Website, unless otherwise expressly specified in the updated version.

1.4. By using the Website, online services and/or otherwise providing their Personal Data to the Controller, the Data Subject confirms that they have read this Policy and understand its provisions. Where Processing of Personal Data is carried out on the basis of the Data Subject's consent, such consent is given explicitly in accordance with Section 2.2 of this Policy.

1.5. Conditions for Processing of Personal Data by the Controller:

1.5.1. Processing of Personal Data is carried out on the basis of one or more legal grounds provided for by Applicable Law (including but not limited to: the Data Subject's consent, necessity for performance of a contract, fulfilment of the Controller's legal obligations, protection of the legitimate interests of the Controller and/or third parties while respecting the rights of the Data Subject, and other grounds provided for by law);

1.5.2. Processing of Personal Data is limited to the achievement of specific, predetermined and lawful purposes; Processing of Personal Data that is incompatible with such purposes is not allowed;

1.5.3. Personal Data processed must be adequate, relevant and limited to what is necessary for the purposes of Processing; the Controller strives to minimize the amount of data collected;

1.5.4. The Controller takes reasonable measures to ensure the accuracy and relevance of Personal Data, as well as to delete or correct inaccurate or outdated data within a reasonable time;

1.5.5. Personal Data is stored no longer than necessary for the purposes for which it is processed, unless a longer storage period is required or allowed by Applicable Law or is conditioned by the need to protect the Controller's legitimate interests (for example, for accounting, tax reporting, dispute resolution, assertion and defence of legal claims).

1.6. On the basis of a contract, the Controller may entrust Processing of Personal Data to Processors (contractors, partners, IT service providers, payment providers, hosting providers, marketing and analytics service providers, etc.), subject to their compliance with confidentiality and Personal Data security requirements, as well as other requirements of Applicable Law.

1.7. Interaction of the Controller with government authorities of the United Arab Emirates and other states is carried out within the competence of such authorities and subject to the existence of legal grounds for requesting and providing the relevant information.

2. LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

2.1. The legal grounds for Processing Personal Data by the Controller, depending on the specific situation, are:

2.1.1. **Consent of the Data Subject** to the Processing of their Personal Data for one or more specific purposes, expressed in a form provided for by Applicable Law and this Policy (including by ticking a checkbox, performing clear conclusive actions, signing a contract, form or other document).

2.1.2. **Necessity for the performance of a contract** to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into such a contract (including conclusion, performance, amendment, support and termination of contracts for the provision of services, corporate support, advertising and other services).

2.1.3. **Fulfilment of the Controller's legal obligations** provided for by Applicable Law, including in the field of accounting, tax regulation, obligations on anti-money laundering and combating financing of terrorism (AML/CFT), sanctions compliance and other regulatory requirements.

2.1.4. **Protection of vital interests** of the Data Subject or another person in cases where Processing of Personal Data is necessary to prevent or eliminate a threat to life and health.

2.1.5. **Necessity for the purposes of the legitimate interests of the Controller or third parties**, subject to conducting a balancing test and documenting such assessment, including: ensuring information and physical security, preventing fraud and abuse, protecting the rights, property and interests of the Controller and/or third parties, carrying out internal administrative operations, except where the interests and fundamental rights of the Data Subject override such interests.

2.1.6. **Other grounds** expressly provided for by Applicable Law and applicable to the Controller's activities.

2.2. The Data Subject's consent may be expressed, in particular, by carrying out one or more of the following actions:

– registration of an account (personal account) on the Website or in the Controller's online services;

– submission of a feedback form, application, request for consultation or other message via the Website, messengers, email or other communication channels of the Controller;

– acceptance of an offer or signing of a contract that directly refers to this Policy and/or a separate consent to Processing of Personal Data;

– ticking a checkbox with text informing about consent to Processing of Personal Data and/or to receiving marketing communications;

– continuing to use the Website in the presence of an appropriate notice on the use of cookies and/or other tracking technologies, if such consent is provided for by Applicable Law.

2.3. The Data Subject has the right to withdraw their consent to Processing of Personal Data at any time if Processing is based on consent, by sending the Controller a corresponding request to the contacts indicated in this Policy. Withdrawal of consent does not affect the lawfulness of Processing carried out prior to such withdrawal.

3. PURPOSES, SCOPE AND RETENTION PERIODS FOR PROCESSING PERSONAL DATA

3.1. The Controller processes Personal Data only for purposes consistent with its business activities (corporate services, advertising, e-commerce and related consulting and support), as well as for the functioning of the Website and online services.

3.1.1. Registration and maintenance of accounts, provision of access to online services

Purpose of Processing: creation and maintenance of User accounts in the Controller's online services, provision of access to the personal account, profile configuration, management of access rights, settings and notifications.

Categories and list of data processed: first name, last name, and, where applicable, patronymic/second name; email address; valid mobile phone number (if provided); login; encrypted password; account identifier; selected interface language and notification settings; history of logins to the account and actions related to authorization; as well as other information voluntarily provided by the User in the profile (including, where applicable, company name, position and other provided data).

Categories of Data Subjects: Users of the Website and the Controller's online services, clients, representatives of corporate clients and partners.

Methods of Processing: collection, recording, systematization, storage, use, updating, blocking, deletion, destruction, as well as transfer to Processors involved in supporting the IT infrastructure, subject to confidentiality.

Processing and retention period: for the duration of the account and/or contract with the Controller and for the period necessary to resolve potential disputes and protect the Controller's legitimate interests, unless a longer period is provided for by Applicable Law.

3.1.2. Processing of requests, enquiries and correspondence

Purpose of Processing: processing incoming requests, enquiries and messages sent via the Website, messengers, email, by phone and other channels, provision of consultations, technical and information support, conduct of business correspondence.

Categories of data: first name, last name, patronymic (if any); contact phone number; email address; company and position (if any); content of the enquiry and attached files (including documents, presentations, other business information); technical metadata of messages (date, time, communication channels).

Categories of Data Subjects: potential and existing clients, partners, representatives of legal entities, Users of the Website and services.

Methods of Processing: collection, recording, systematization, accumulation, storage, analysis, use, transfer within the Controller and to Processors involved in processing requests (for example, providers of ticketing systems and CRM), blocking, deletion, destruction.

Retention period: until the purposes of Processing are achieved and for the period necessary to document the consultations provided, perform contractual obligations and resolve disputes (as a general rule, not less than the limitation period established by Applicable Law).

3.1.3. Conclusion and performance of contracts, financial settlements

Purpose of Processing: conclusion, performance, amendment and termination of contracts with natural persons and legal entities (including corporate support, advertising, e-commerce and related services), conduct of settlements, recording of payments, issuance of invoices, acts and other documentation.

Categories of data: first name, last name, and, where applicable, patronymic; contact details of clients and their representatives (email address, phone number); details of concluded contracts and appendices thereto; payment details (data of bank accounts, cards, electronic wallets or other payment instruments used for settlements in respect of the Controller's services); tax and accounting information; information and copies of registration and constituent documents of legal entities, powers of attorney and other documents confirming representatives' authorities.

Categories of Data Subjects: natural person clients; representatives and employees of corporate clients and partners; representatives of suppliers and contractors.

Methods of Processing: collection, recording, systematization, accumulation, storage, use, updating, transfer to Processors (banks and payment organisations, accountants, auditors, providers of electronic document management services), blocking, deletion, destruction, subject to the requirements of Applicable Law.

Retention period: for the duration of the contract and for the period necessary for accounting and tax purposes and for protecting the rights and legitimate interests of the Controller (usually at least the period established by legislation on accounting and taxation).

3.1.4. Identification and verification of clients (KYC/AML/CFT), compliance with regulatory requirements

Purpose of Processing: identification and verification of clients in order to fulfil requirements of Applicable Law in the field of anti-money laundering, combating financing of terrorism, sanctions control and other regulatory requirements; risk assessment and management.

Categories of data: first name, last name, patronymic; date of birth; citizenship; photographs and copies of official identification documents (passport, national ID, driving licence, etc.); residential and/or registration address; information on place of work and position; tax identification number (if applicable); information on source of funds, beneficial owners and ownership structure; data on inclusion in sanctions lists; other information directly provided for by Applicable Law and/or required by banks and other counterparties for compliance procedures.

Categories of Data Subjects: natural person clients; beneficial owners, managers and representatives of corporate clients; other persons subject to identification in accordance with Applicable Law.

Methods of Processing: collection, recording, storage, verification, comparison with open sources and databases, transfer to banks, payment providers and other entities involved in compliance checks, to the extent necessary to comply with legal requirements and contractual obligations.

Retention period: for the period established by Applicable Law for storage of KYC/AML documents (including possible minimum storage periods after termination of the relationship with the client).

3.1.5. Marketing communication, information about services and events

Purpose of Processing: sending information and marketing messages to Users and clients (newsletters, information about new products, services, special offers, webinars, events), carrying out surveys and satisfaction studies.

Categories of data: first name, last name; email address; phone number; account identifier (if the mailing is sent to a User registered in the Controller's online services); information on the fact of receipt, opening and clicking links in marketing messages; belonging to certain segments or categories of clients; preferences specified by the User in relation to mailings and communication channels.

Categories of Data Subjects: subscribers to mailings; clients and Users who have provided their contact details and consent to receiving messages; representatives of corporate clients and partners.

Methods of Processing: collection, recording, storage, use for preparing and sending mailings, transfer to providers of email marketing services and messenger platforms, analysis of communication effectiveness, blocking, deletion, destruction.

Retention period: until withdrawal of consent to receiving marketing messages and/or objection to Processing of Personal Data for the respective purposes, and for a reasonable period after withdrawal in order to document compliance with legal requirements (for example, to confirm the fact of unsubscribe and absence of further mailings).

3.1.6. Use of cookies, web analytics and improvement of the Website

Purpose of Processing: ensuring proper functioning of the Website, adapting the display and functionality to the User's device and preferences, ensuring security, maintaining visit statistics, analysing User behaviour for improving the Website and services, as well as displaying relevant content and offers.

Categories of data: IP address; browser and operating system data; language settings; device and screen resolution; information about sessions, time of visits, pages viewed and actions on the Website; cookie identifiers and other online identifiers; referrer pages; other technical data provided by the browser or device.

Categories of Data Subjects: all Users visiting the Website.

Methods of Processing: collection, recording, systematization, storage, use, analysis, anonymization, aggregation, transfer to providers of web analytics, advertising and marketing platforms (to the extent and on the conditions consistent with Applicable Law and agreements with such providers).

Retention period: the lifetime of individual cookies (determined by their type and the User's browser settings) and the period necessary to achieve the purposes of Processing. The User may manage cookies via browser settings and, where available, via the Website interface (cookie consent banner/panel), understanding that disabling certain types of cookies may limit the Website's functionality.

The Controller uses various types of cookies: strictly necessary, functional, analytical and marketing. Use of marketing and analytical cookies is carried out only after obtaining the User's explicit consent via the cookie banner at the first visit to the Website. The User may withdraw consent or change cookie settings at any time through the cookie management interface on the Website.

3.1.7. Ensuring security, prevention of fraud and protection of the Controller's rights

Purpose of Processing: ensuring information and physical security, prevention of fraudulent and other unlawful actions, protection of the rights, interests and property of the Controller, its clients and third parties, as well as fulfilling requirements of Applicable Law regarding data security.

Categories of data: account data; system log files; information on the User's actions in the services; technical information (IP address, device data, session identifiers); information on suspicious operations and incidents; correspondence related to security.

Categories of Data Subjects: Users, clients, representatives of counterparties, as well as persons suspected of unlawful actions in relation to the Controller, its clients and services.

Methods of Processing: collection, recording, systematization, storage, analysis, comparison, transfer to competent government authorities and security partners (for example, providers of anti-fraud services), blocking, deletion, destruction.

Retention period: until the purposes of Processing are achieved, as well as for the period necessary to establish, exercise or defend legal claims in relation to the relevant incidents.

3.1.8. Automated Processing and profiling

Purpose of Processing: automated analysis and evaluation of certain personal aspects of Data Subjects for personalization of offers, fraud risk assessment, improvement of service quality.

Categories of data: history of actions on the Website and in the services; data on transactions and use of services; technical and behavioural metrics; preferences and interests identified on the basis of interaction with content.

Categories of Data Subjects: registered Users, clients, Website visitors.

Methods of Processing: automated analysis using algorithms and machine learning models; categorization and segmentation; formation of personalized offers.

Notification and rights of Data Subjects: the Controller informs Data Subjects about the existence of Automated Processing, including profiling, the logic of its operation, significance and possible consequences of such Processing. The Data Subject has the right not to be subject to decisions based solely on Automated Processing (including profiling) which produce legal effects concerning them or similarly significantly affect them, except where such decision:

– is necessary for entering into, or performance of, a contract between the Data Subject and the Controller;

– is authorised by Applicable Law with appropriate safeguards for the Data Subject's rights;

– is based on the Data Subject's explicit consent.

In cases of automated decision-making, the Controller ensures the possibility for the Data Subject to obtain explanations and to challenge the decision.

4. COLLECTION, PROCESSING, STORAGE, PROTECTION, TRANSFER AND DESTRUCTION OF PERSONAL DATA

4.1. Procedure and conditions of Processing

4.1.1. Processing of Personal Data is carried out by the Controller in compliance with the principles of lawfulness, fairness, transparency, purpose limitation and data minimisation, as well as other principles provided for by Applicable Law.

4.1.2. The Controller may process Personal Data both by automated means and without the use of automation (on paper), depending on the purposes of Processing and internal procedures applied.

4.1.3. The Controller processes Personal Data only to the extent and for as long as necessary to achieve specific purposes of Processing and to fulfil its obligations towards Data Subjects and counterparties, unless another retention period is established by Applicable Law or follows from the Controller's legitimate interests.

4.1.4. In the event of withdrawal of consent, objection to Processing or exercise of the Data Subject's rights, the Controller terminates the respective Processing, except where Applicable Law allows or obliges Processing to continue without consent, in particular for the purposes of complying with legal obligations or protecting the rights and legitimate interests of the Controller.

4.1.5. Upon achievement of the purposes of Processing, expiration of retention periods or loss of the need for Processing, the Controller deletes or anonymizes Personal Data within a reasonable time, unless further storage is required by law or for the protection of the Controller's rights.

4.2. Measures for protection of Personal Data

4.2.1. The Controller takes reasonable and sufficient organizational, technical and physical measures to protect Personal Data against unauthorised or unlawful access, alteration, disclosure, use, destruction, loss or other unlawful forms of Processing.

4.2.2. The protection measures applied by the Controller may include: access control to systems and databases; use of encryption and secure communication channels; deployment of firewalls and intrusion detection systems; monitoring and analysis of information security events; backup and recovery of data; regular updating of software and anti-virus protection; training of employees on confidentiality and data protection; implementation of internal security policies and procedures.

4.2.3. The Controller ensures that Processors engaged in Processing of Personal Data adopt protection measures that are at least as effective and comply with confidentiality requirements in accordance with contracts and Applicable Law.

4.2.4. The Controller shall not be liable for the security of Personal Data of another party to the extent that the Data Subject independently discloses their information to third parties or uses third-party websites, services and applications which may be linked to from the Website. The Data Subject must independently familiarize themselves with the privacy and data processing policies of such third parties.

4.3. Transfer of Personal Data to third parties and Cross-border Transfer

4.3.1. The Controller may transfer Personal Data to third parties in the following cases:

– to persons acting on behalf of or under the instruction of the Controller as Processors (providers of IT services, hosting, CRM systems, payment providers, providers of marketing and analytics services, legal advisers, auditors, etc.), provided that appropriate contracts are concluded and such persons comply with confidentiality and security requirements;

– to banks, payment organisations, financial service providers for the purpose of executing payments, refunds, checks and other operations provided for by contracts with the Data Subject;

– to government authorities and regulators of the UAE and other states where there are legal grounds for a request and to the extent provided for by Applicable Law (including financial monitoring authorities, tax, law enforcement and judicial authorities);

– to persons providing legal protection services to the Controller, representing its interests in courts and other bodies, for the purpose of protecting the Controller's rights and legitimate interests;

– in aggregated and anonymized form for conducting analytical research, statistics, development and improvement of products and services. Such information does not allow identification of a specific Data Subject;

– to other third parties where the Data Subject has explicitly consented to such transfer or where such transfer is directly provided for by Applicable Law.

4.3.2. The Controller may carry out Cross-border Transfer of Personal Data to servers located outside the UAE, as well as provide remote access to Personal Data from other countries, subject to one of the following conditions:

– the recipient country is included in the list of countries with an adequate level of Personal Data protection approved by the UAE Data Office;

– standard contractual clauses approved by the competent UAE authority have been concluded;

– explicit consent of the Data Subject to Cross-border Transfer has been obtained after informing them about possible risks;

– the transfer is necessary for the performance of a contract between the Controller and the Data Subject;

– the transfer is carried out within the framework of binding corporate rules approved by the UAE Data Office.

4.3.3. Where Processing of Personal Data is entrusted to a Processor, the Controller:

– concludes a contract with such Processor defining the subject matter, purposes, nature and duration of Processing, types of Personal Data, categories of Data Subjects, security requirements and conditions for return or destruction of Personal Data upon completion of Processing;

– ensures that the Processor Processes Personal Data only within the documented instructions of the Controller and does not use it for its own purposes unless otherwise explicitly agreed with the Data Subject.

4.4. Sources of obtaining Personal Data

4.4.1. As a general rule, Personal Data is provided by the Data Subject to the Controller directly (when registering on the Website, filling out forms, entering into a contract, sending requests, etc.).

4.4.2. In certain cases, the Controller may obtain Personal Data from other sources, if this is permitted by Applicable Law, in particular:

– from corporate clients and partners with regard to their employees and representatives indicated in contracts and as contact persons;

– from providers of payment and fintech services to the extent necessary for execution of operations;

– from open sources and public registers for the purposes of information verification, fulfilment of AML/sanctions screening requirements and ensuring compliance;

– from third parties acting on behalf of the Data Subject (for example, authorised persons or intermediaries), provided they have the necessary authority.

5. RIGHTS OF DATA SUBJECTS, OBLIGATIONS OF THE CONTROLLER AND DATA SUBJECTS

5.1. Rights of the Data Subject

5.1.1. To the extent provided for by Applicable Law, the Data Subject has the right to:

– receive from the Controller confirmation as to whether or not their Personal Data is being Processed and information regarding such Processing;

– request access to their Personal Data, including obtaining a copy of the data Processed by the Controller;

– request clarification, rectification and updating of their Personal Data if it is inaccurate or incomplete;

– request deletion (erasure) of their Personal Data in cases provided for by Applicable Law (for example, where the data is no longer necessary for the purposes for which it was collected, or the Data Subject has withdrawn consent and there are no other legal grounds for Processing);

– request restriction of Processing of Personal Data (for example, for the period of verification of data accuracy or lawfulness of Processing);

– object to Processing of Personal Data for specific purposes, including direct marketing, at any time;

– receive their Personal Data in a structured, commonly used and machine-readable format and, where technically feasible, request transmission of such data to another controller (right to data portability);

– not be subject to decisions based solely on Automated Processing, including profiling, if such decisions produce legal effects concerning the Data Subject or similarly significantly affect them, except in cases expressly provided for by Applicable Law;

– withdraw consent to Processing of Personal Data where Processing is carried out on the basis of consent;

– lodge a complaint with the competent supervisory authority of the UAE in the field of Personal Data or another authorised body in case of violation of their rights, and seek judicial protection.

5.1.2. The Data Subject exercises their rights by sending a written or electronic request to the Controller's contact details specified in Section 8 of this Policy. The Controller may request additional information necessary to confirm the identity of the applicant and prevent unauthorised access to data.

5.1.3. The Data Subject may at any time refuse to receive marketing communications and/or change their preferences regarding mailings and use of cookies by using the respective links in electronic messages, account settings (if applicable), the Website interface or browser settings. Refusal of marketing communications does not affect receipt of service and other mandatory notifications related to provision of the Controller's services.

5.1.4. The Controller undertakes to consider the Data Subject's request and provide a response within 30 (thirty) calendar days from the date of receipt of the request and confirmation of the applicant's identity. If it is necessary to extend the consideration period (by no more than 30 additional days), the Controller shall inform the Data Subject of the reasons for the delay.

5.2. Obligations of the Controller

5.2.1. The Controller shall:

– process Personal Data in accordance with Applicable Law and this Policy;

– provide the Data Subject with the necessary information on the Processing of Personal Data in an understandable and accessible form;

– ensure the accuracy, relevance and sufficiency of Personal Data being Processed;

– apply appropriate organizational and technical measures to protect Personal Data;

– in the event of a Personal Data breach which may lead to a risk to the rights and freedoms of Data Subjects, notify the UAE Data Office no later than 72 hours from the moment of detection of the breach, unless a different period is established by applicable regulations;

– notify affected Data Subjects of a significant Personal Data breach without undue delay if such breach may result in a high risk to their rights and freedoms;

– cooperate with supervisory authorities in the field of Personal Data protection;

– consider requests and enquiries of Data Subjects within the time limits and in the manner established by law;

– cease Processing and/or delete Personal Data in cases and within the time limits provided for by Applicable Law and this Policy.

5.3. Obligations of the Data Subject

5.3.1. The Data Subject shall:

– provide the Controller with accurate, correct and up-to-date information about themselves to the extent necessary to achieve the purposes of Processing;

– promptly inform the Controller of any changes to their Personal Data (for example, contact information, document details, representative status);

– not violate the rights and legitimate interests of third parties when providing their Personal Data to the Controller, and provide such data only where there are necessary grounds and authority;

– comply with the terms of contracts and rules for using the Website and the Controller's online services, including compliance with information security requirements;

– upon detecting facts of compromise of their account, unauthorized access to it or suspected leakage of their Personal Data, immediately notify the Controller via the contacts specified in this Policy.

6. LIABILITY

6.1. The Controller is liable for compliance with the requirements of Applicable Law in the field of Personal Data protection and this Policy to the extent established by such law.

6.2. For violation of the rules for Processing Personal Data, unlawful disclosure, loss, destruction or other violations of the rights of Data Subjects, the Controller and/or its officers may be held liable in accordance with Applicable Law, and may be obliged to compensate the Data Subject for damage in cases and to the extent established by law.

6.3. The Data Subject understands and agrees that in the event of providing inaccurate, incomplete or outdated information, the Controller shall not be liable for consequences arising from the use of such information, as well as for the impossibility of properly providing services.

6.4. The Controller is not liable for the actions of third parties to whom the Data Subject independently discloses their data or with whom they interact through external websites and services, even if links to such websites and services are placed on the Controller's Website.

7. FINAL PROVISIONS

7.1. This Policy and relations related to Processing of Personal Data by the Controller are governed by the laws of the United Arab Emirates, unless otherwise directly follows from mandatory rules of law or agreements with Data Subjects.

7.2. The Controller is entitled unilaterally to amend this Policy where necessary to align it with changes in Applicable Law, the Controller's internal procedures or the functionality of the

Website and services. The Controller recommends that Data Subjects periodically acquaint themselves with the current version of the Policy on the Website.

7.3. In the event of a conflict between the provisions of this Policy and the terms of a specific contract with a Data Subject, the provisions of such contract shall prevail, provided this does not contradict Applicable Law.

7.4. Issues not regulated by this Policy are governed by Applicable Law, as well as by the Controller's internal documents adopted to further develop requirements on Personal Data protection and confidentiality.

7.5. The Controller's services are not intended for independent use by persons under the age of 21 (in accordance with UAE civil majority legislation) without the consent of their legal representatives, except for emancipated persons in accordance with applicable law. The Controller does not knowingly collect or process Personal Data of minors without documented consent of parents or legal guardians. If it is discovered that Personal Data of a minor has been obtained without the necessary consent, the Controller undertakes to cease Processing and delete such data within 14 (fourteen) calendar days from the moment of discovery, unless further retention is required by Applicable Law.

7.6. The effective date of this Policy is the date of its publication on the Website. Document version: 1.0. Date of last update: **..**2025. The history of amendments to this Policy is available upon request of Data Subjects to the contact address specified in Section 8.

8. CONTROLLER DETAILS

MAIZON GROUP L.L.C-FZ
License Number: 2423151.01
Registered / Office Address:
Meydan Grandstand, Meydan Road, Nad Al Sheba,
6th Floor, Dubai, United Arab Emirates
Contact details:
Website: www.maizongroup.com/ru
E-mail: info@maizongroup.com
For exercising Data Subjects' rights and sending enquiries regarding Processing of Personal Data:
E-mail: privacy@maizongroup.com
Data Subjects are also entitled to lodge a complaint with the UAE Data Office (https://dataoffice.gov.ae) in case of violation of their rights in the field of Personal Data protection.
Phones: +971 50 693 0343 (UAE) / +357 95 903 806 (Cyprus)