Privacy Policy www.dbstore.online

The present information on the protection of personal data ("Privacy Policy") governs the treatment of personal data carried out through the website managed by Etabeta Ltd, a company established in accordance with the legislation of Malta, with legal headquarters in via 3, Advance Business Centre, Triq Guze Flores, Santa Venera, P.IVA MT30678428 (following, also "Titolare del trattamento" or simply "Titolare").

The Owner acts in respect of the principles established by the European and international norms applicable in the matter of personal data protection, guaranteeing an adequate level of protection of the rights and freedoms of the interested parties, even in the case of transfer of data to third countries, where applicable.

2. Typologia di dati trattati

Within the scope of the provision of online services, the Owner collects and treats the following categories of personal data, conferred directly by the interested party via the website or collected within the contractual relationship:

Identification and contact data: name, surname, email address, telephone number and other data useful for identifying or contacting the physical person representing the applicant company.

Company data: denominazione o ragione sociale, legal headquarters, numero di partita IVA, and other data of commercial registration of the company.

Documentazione aziendale: copia aggiornata della visura camerale or equivalent documento di registration a un registro ufficiale delle imprese, come prova dell'esistenza legale dell'entita juridica.

Data of the legal representative: if requested, a copy of the identity document of the owner or the legal representative of the company, necessary to verify the identity and authority of the representative.

Fiscal and administrative data: information necessary to fulfill fiscal and accounting obligations, including billing addresses, fiscal codes and bank details eventually supplied.

Tutti i dati vengono trattati nel rispetto dei principi di liceità, correttezza, trasparenza, pertinenza e minimizzazione. Il conferimento di alcuni dati podrème essere obbligatorio per acceder al servizio o per l'empimento di obligazione legali; in tali casi, il mancato conferimento podrème comportare l'impossibilità di erogare i servizi prereturi.

3. Purpose of processing and legal bases

The personal data collected will be processed for the following purposes:

Responding to requests for information (legal basis: execution of pre-contractual measures)

Administrative and tax management of business relationships (legal basis: legal obligation)

Verifying company requirements using official documentation (legal basis: legitimate interest of the Data Controller)

Possible requests for identification documents for security purposes and prevention of abuse (legal basis: legitimate interest of the Data Controller)

4. Processing methods

The Data Controller processes personal data in full compliance with the principles of lawfulness, fairness, transparency, integrity, and confidentiality, as required by Regulation (EU) 2016/679 (GDPR) and the harmonized Maltese national legislation.

Personal data is processed using electronic, digital, and paper-based tools, lawfully and proportionately, using methods strictly related to the purposes for which they were collected,

adopting appropriate technical and organizational measures to ensure their security and prevent their loss, unlawful use, unauthorized access, disclosure, or modification.
Specifically, the Data Controller adopts measures such as:
Data access permitted only to authorized, previously trained individuals;
Authentication, encryption, and access logging systems;
Administrative access control and tracking;
Secure protocols for data transmission and exchange;
Periodic audits of infrastructure and procedures;
Automatic backups and redundancy of critical data.
Data is stored on servers located primarily in European Union member countries. However, in managing digital services, the Data Controller may use external providers—including cloud service providers, SaaS (Software as a Service) technologies, and IT infrastructure—who may process data in third-party countries.
In such cases, all processing by these entities will take place exclusively as data processors, subject to the signing of specific contractual agreements that include:
the adoption of standard contractual clauses (SCCs) approved by the European Commission, or other equivalent safeguards (e.g., Binding Corporate Rules),
accompanied, where necessary, by additional technical measures (e.g., end-to-end encryption, pseudonymization, territorial access controls) and impact assessments (TIA).
No automated decision-making or significant profiling is envisaged on the data processed, with the exception of marketing activities performed exclusively with prior consent.
5. Data Retention
The Data Controller retains the personal data collected for a limited period, proportionate and consistent with the purposes for which they were collected, in compliance with the principles of integrity, availability, and accountability. The data is processed and archived for the entire duration of the contractual or commercial relationship with the client company.
Specifically:
Data of active customers: All personal and business data collected will be retained for the entire duration of the contractual relationship, i.e., for as long as the service provided by the Data Controller is active for the interested company. Processing is necessary for the provision of the service and to fulfill related contractual, administrative, and legal obligations.
Invoicing and tax compliance data: retained for a period of no less than 10 years from the termination of the relationship, as required by applicable tax and accounting regulations.
Data collected via contact forms (non-customers): In the absence of subsequent formalization of the commercial relationship, the data will be retained for a maximum of 24 months from the date of collection.
Identification documentation of the legal representative: retained only for the time necessary to complete the required checks, and in any case no longer than 12 months, unless extensions are justified by legal or anti-fraud requirements.
Data for marketing purposes: If the data subject has provided specific consent, this data will be retained for up to 36 months from collection or until consent is revoked, whichever occurs first.
Data of former customers or inactive accounts: Upon termination of the business relationship, data no longer required will be retained for a maximum period of 5 years from the termination of

the service, exclusively for legal purposes (e.g., legal defense, tax audits) and subsequently deleted or anonymized.
All data will be deleted or permanently anonymized upon expiration of the aforementioned terms, unless regulatory obligations require further retention.
6. Disclosure to third parties and dissemination of data
The Data Controller guarantees that the personal data processed will not be transferred or disclosed to third parties for commercial, promotional, or profiling purposes, except to the extent expressly authorized by the data subject or required by applicable law.
Disclosure of data to third parties is permitted exclusively in the following cases:
Compliance with legal and regulatory obligations, including tax, accounting, or corporate obligations, which require the disclosure of data to competent authorities, public bodies, or supervisory bodies;
Performance of the contract or management of activities related to the business relationship, for which the data may be disclosed to third parties such as:
tax and legal advisors;
providers of administrative, banking, and accounting services;
technology partners and hosting companies or cloud providers who provide technical and IT support for the website and company infrastructure;
providers of IT security and fraud prevention services;
Defense of a right in court, where necessary.
All the third parties listed above act, where applicable, as data processors, pursuant to specific contractual agreements that govern access, processing methods, and the security measures adopted, in compliance with international standards and the principle of accountability.
The updated list of external parties to whom data may be disclosed is available upon written request to the Data Controller.
Under no circumstances will personal data be disseminated indiscriminately, or communicated to unspecified parties, nor will they be published or made accessible to an indefinite number of parties, except as required by law or with express authorization.
7. International data transfer
The Data Controller hereby informs you that the personal data processed may, where necessary, be transferred to countries outside Malta. Such transfers will take place exclusively in accordance with applicable regulations and in the presence of adequate safeguards.
In particular:
To countries of the European Union and the European Economic Area (EEA): transfers are made freely, as these countries guarantee a level of protection compliant with European standards. Pursuant to Maltese national legislation, prior notification to the Maltese Data Protection Authority is required.
To third countries with an adequacy decision: data may be transferred to countries for which the European Commission has adopted an adequacy decision pursuant to Article 45 of the GDPR, or which have been recognized as adequate by the competent Maltese Authority.
To other third countries: in the absence of an adequacy decision, transfers are permitted exclusively in compliance with the safeguards provided for by Articles 15 et seq. 46 and 47 of the GDPR and local legislation, including:
Standard Contractual Clauses (SCC);

Binding Corporate Rules (BCR);
Adoption of additional technical measures (e.g., encryption, pseudonymization, audits);
Transfer Impact Assessments (TIA), where required.
To NATO member countries: Following the regulatory change of May 14, 2025, Malta allows transfers to NATO member countries under a preferential regime, equivalent to that of EEA countries. Such transfers require simple notification to the local authority and the adoption of minimum documentable guarantees.

8. Rights of Data Subjects

In accordance with applicable data protection legislation, in particular Regulation (EU) 2016/679 (GDPR), data subjects, i.e., natural persons whose personal data is processed by the Data Controller, have the right to exercise the following rights at any time:
Right of access: obtain confirmation as to whether or not personal data concerning them is being processed and, where that is the case, access to that data and receive information regarding the purposes of the processing, the categories of data processed, the recipients, the retention periods, the source of the data (if not collected directly from the data subject), the existence of automated decision-making processes, and the safeguards adopted in the event of international data transfer.
Right of rectification: obtain the correction of inaccurate personal data or the completion of incomplete personal data.
Right to erasure ("right to be forgotten"): request the erasure of personal data in the cases provided for by law, for example, when the data is no longer necessary for the purposes for which it was collected or processed, or in the event of withdrawal of consent where there is no other legal basis.
Right to restriction of processing: obtain restriction of processing under specific conditions (e.g., contesting the accuracy of the data, objecting to processing, unlawful processing as an alternative to erasure).
Right to data portability: receive the personal data provided to the Data Controller in a structured, commonly used, and machine-readable format and transmit that data to another controller, where technically feasible, if the processing is based on consent or a contract and is carried out by automated means.
Right to object: object, in whole or in part, to the processing of personal data for legitimate reasons relating to the data subject's particular situation, including processing based on the Data Controller's legitimate interests. This right also extends to any use of the data for direct marketing purposes.
Right not to be subject to automated decisions, including profiling, that produce legal effects or significantly affect you, except as provided by law.
Right to lodge a complaint: You have the right to lodge a complaint with a supervisory authority competent in the country where you habitually reside, work, or where the alleged infringement occurred.

9. Changes to this Privacy Policy

The Data Controller reserves the right to update, modify, or supplement this Privacy Policy at any time to reflect any regulatory changes, developments in case law, technological advances, or changes in the methods of processing personal data.

Any substantial changes that significantly impact the rights and freedoms of data subjects will be duly notified via a specific notice on the website or, where applicable, directly to registered users.
Users are therefore encouraged to periodically consult this section to review the most up-to-date version of the Privacy Policy, which is always available on the Data Controller's official website. The date of the last update will be shown at the bottom of this document.

10. Contact Information
For any requests, information, or clarifications regarding the processing of personal data, as well as to exercise the rights granted to data subjects (access, rectification, erasure, objection, portability, restriction of processing), you can contact the Data Controller at the following addresses:
Data Controller:
Etabeta Ltd
Registered Office: Via 3, Advance Business Centre, Triq Guze Flores, Santa Venera
VAT No.: MT30678428
Email for privacy inquiries: privacy@dbstore.online
Contact form: available on the official website www.dbstore.online
The Data Controller undertakes to respond to requests within the timeframes established by applicable law and to cooperate in full transparency with the competent supervisory authorities.

APPENDIX

Safeguards Adopted for the International Transfer of Personal Data

In accordance with Regulation (EU) 2016/679 (GDPR), Etabeta Ltd., as Data Controller, adopts a series of technical, organizational, and contractual safeguards to ensure an adequate level of protection when transferring personal data to third countries, i.e., outside the European Economic Area (EEA).

1. Standard Contractual Clauses (SCCs)

In the event that personal data is transferred to entities established in countries not subject to an adequacy decision by the European Commission, the Data Controller adopts the Standard Contractual Clauses approved by the Commission pursuant to Article 46 of the GDPR as the legal basis for the transfer.

These clauses govern the relationship between the data exporter and the data importer and contain specific obligations to ensure:

the adoption of adequate security measures;

respect for the rights of data subjects;

the handling of requests from public authorities;

Effective recourse and accountability mechanisms.

2. Additional technical and organizational measures

In addition to contractual clauses, Etabeta Ltd. adopts additional measures to strengthen data protection, including:

Encryption of personal data in transit and at rest;

Pseudonymization where applicable;

Limiting access to authorized individuals;

Monitoring and logging of data access;

Periodic security audits of suppliers;

Internal policies for the classification and protection of information.

3. Transfer Impact Assessment (TIA)

In accordance with the EDPB (European Data Protection Board) guidelines, the Data Controller conducts a transfer impact assessment (TIA) to analyze:

the regulatory environment of the third country of destination;

the potential risks to the rights of data subjects;

the additional measures to be adopted to ensure protection equivalent to that of the EU.

4. Accountability and Transparency

Etabeta Ltd maintains detailed documentation relating to transfers, including contracts, impact assessments, and the technical measures adopted. Data subjects may request a copy of the safeguards applicable to the transfer by contacting the Data Controller through official channels.

This annex is an integral part of Etabeta Ltd's Privacy Policy and is updated periodically based on regulatory and technical developments.