Data Processing Agreement

MIBO TRADE IMPORT EXPORT SRL · Version 2, dated 10 November 2026

1. The parties and the words used

1.1. MIBO TRADE means MIBO TRADE IMPORT EXPORT SRL, with its registered office in Iași, Strada Bucium nr. 57A, județul Iași, CUI (tax identification number) 36438576, VAT code RO36438576, Trade Register no. J22/2367/2020, share capital 200 lei, e-mail office@cateruno.ro, the firm that makes and operates Cateruno.

1.2. The Firm means the firm that has an account in Cateruno, _____, CUI _____, whatever its form (company, authorised natural person, sole proprietorship or family business). The person who accepts the agreement declares that they have the right to bind the Firm (article 3.4 of the Terms).

1.3. The Terms means the Cateruno Terms and Conditions, which also include the early access conditions (chapter 5 of the Terms). The agreement forms part of the Terms (article 1.4 of the Terms). Capitalised words not defined here, such as the Platform, the Owner, the Authorised Persons, the Accountant, the Firm's Clients, the Firm's Staff, Early Access, the Launch, the Subscription, the Free Trial and Account Closure, have the meaning in article 2.1 of the Terms.

1.4. GDPR means Regulation (EU) 2016/679. The words "personal data", "processing", "controller", "processor", "data subject", "profiling" and "personal data breach" have the meaning in Article 4 GDPR. Incident means a breach of the security of the Firm's Data.

1.5. The Firm's Data means the personal data that the Firm, the Authorised Persons, the Firm's Clients or the Firm's Staff enter, upload or send through the Platform and the data that the Platform produces from it. It is described in Annex A.

1.6. Sub-processor means another processor that MIBO TRADE uses to process the Firm's Data (Article 28(2) and (4) GDPR).

1.7. For the Firm's Data, the agreement takes precedence over the rest of the Terms (article 1.4 of the Terms). The rest of the relations between the parties, including the price and the availability of the Platform, are established by the Terms.

1.8. Future features. The rows in the annexes marked "later" describe features that are not active on the date of this version. Their description does not authorise any processing before the contractual, information and security conditions are met; activation follows article 16.1 and, for a new provider, chapter 9.

2. The roles

2.1. For the Firm's Data, the Firm is the controller: it decides why and how it uses the data, for example which clients it enters, which quotes and contracts it sends and whom it calls to events. MIBO TRADE is the processor that processes the data on behalf of the Firm, in accordance with Article 28 GDPR.

2.2. MIBO TRADE is a controller, not a processor, for the data it uses in its own name: the accounts of the Authorised Persons (logging in, two-step verification, security and technical logs), early access requests, news by e-mail, invoicing of the Subscriptions (from the Launch), proof of acceptance of the Terms, the handling of notices about illegal content and of requests for re-examination, and the management of support requests sent to office@cateruno.ro. For this data, the privacy notice for the app's accounts and the privacy notice on cateruno.ro apply, not this agreement. The Firm's Data included in a support request remains subject to this agreement, and MIBO TRADE removes the information that is not necessary.

2.3. The actions of the Authorised Persons in the Firm's account are part of the Firm's Data. The Firm establishes access and roles. The employed Accountant works under the authority of the Firm; the external accountant may be a processor for the operations carried out on its behalf and a separate controller for their own legal obligations. The classification and the corresponding contract are established according to the actual activity, not solely according to the name of the profession.

2.4. The services that the Firm uses or connects to the Platform on its own are the Firm's, not sub-processors of MIBO TRADE; for them, the Firm has its own contracts and is responsible. These are: the e-mail addresses to which clients reply; WhatsApp and the SMS app, when a message pre-written by the Platform is sent from the Firm's phone; the Firm's Oblio or SmartBill account, through which it issues invoices from the Platform, with its own API key; and, after they are activated, the calendar in which the Firm adds the Platform's calendar link and its account for card payments (2.6). MIBO TRADE transmits data to them only when the Firm requests it through the Platform.

2.5. Stripe, through which MIBO TRADE will collect the Subscriptions from the Launch, and SmartBill, through which MIBO TRADE will issue its invoices to the Firm, work for MIBO TRADE, with the Firm's billing data. They do not receive the data of the Firm's Clients, of guests or of the Firm's Staff.

2.6. Card payment by the Firm's Clients (later, after activation). On the Firm's instruction, MIBO TRADE transmits to the payment service provider contracted by the Firm the data strictly necessary for the transaction and processes the confirmations of the transaction as a processor. NETOPIA acts as an independent controller for the payment service's own purposes and its legal obligations; these operations do not constitute subcontracting of the processing by MIBO TRADE. Any separate activity as a processor is documented in accordance with the actual contract and Article 28 GDPR. The list of recipients indicates the entity, the purpose, the data, the countries and the provider's information notice. Data about allergies, individualised menus and other information unnecessary for payment is not transmitted. Until activation, the Platform does not transmit data to a payment service provider.

3. Subject matter, purposes and duration

3.1. MIBO TRADE processes the Firm's Data only to provide the Firm with the Platform and its features, described in Annex A, plus what is necessary for the Platform to run securely: hosting, backups, protection against abuse, fixing errors and the help requested by the Firm.

3.2. The processing lasts as long as the Firm uses the Platform and, after that, until the deletion in chapter 15.

3.3. MIBO TRADE does not sell the Firm's Data and does not use it for advertising or for training AI models. For this data, it uses only providers that process it solely for the contracted service. For AI providers, the contractual prohibition on training and the evidence of it are shown in Annex C; an AI feature for which the evidence is missing remains switched off. Service data that a provider lawfully processes for its own purpose is identified separately, with the corresponding role and legal basis; this clause does not authorise the reuse of the Firm's content.

3.4. MIBO TRADE may produce anonymous statistics for the administration of the service only through a documented aggregation process that prevents the reasonable identification of persons, including by combination with other information. Removing the name, on its own, is not anonymisation. The Firm's identifiable or pseudonymised data is not reused for MIBO TRADE's own purposes of marketing, commercial analysis or general product improvement. Such use requires a prior analysis of MIBO TRADE's own role as controller, of the legal basis, of the compatibility of the purpose and of informing the persons concerned; a formal contractual instruction does not change the real role. On the date of this version, MIBO TRADE keeps only daily counts for the entire Platform (access requests received and approved, accounts activated, firms active in the last 7 and 30 days, quotes sent and contracts signed, excluding demo data), without names, addresses or other data about persons; the record of the days on which a firm was active is deleted after 30 days.

3.5. AI catalogue import. On the date of this version, the only active AI feature is the import of the catalogue from photos and PDFs: an AI system reads the file uploaded by the Owner or by a manager and proposes items (name, category, description, price, unit, allergens), which an authorised user checks and expressly saves; until they are saved, nothing is written to the catalogue. The file must contain only the catalogue, without data about clients or other persons, without information about the allergy of an identifiable person and without medical documents; if such a file cannot be prepared, the items are entered manually. Before sending, the Platform displays the information about AI and asks for confirmation that the file has been checked. The file is deleted from the Platform's file storage immediately after reading. The providers, countries and retention are in Annexes C, D and E.

3.6. What does not reach AI. Clients' messages, free-text fields in enquiries and in the portal, the client's wishes and health data are not sent to an AI service. Any other AI feature, including the voice assistant and the menu proposal, is activated only after the annexes are completed (the provider, the data, the countries, retention, the training prohibition and the transfer mechanism), the persons concerned are informed and the procedure in chapter 9 is carried out. Extending the data set sent to AI requires a new legal and technical review before activation.

4. The Firm's instructions

4.1. MIBO TRADE processes the Firm's Data only on the basis of the Firm's documented instructions (Article 28(3)(a) GDPR). The instructions are: this agreement, the rest of the Terms, the way in which the Authorised Persons use the Platform (what they enter, what they send, what they delete, what access they give), the Firm's settings in the Platform (for example the roles, the features switched on and the retention periods chosen from Annex E) and the written requests sent by the Owner, from their account address, to office@cateruno.ro.

4.2. For instructions that require manual intervention, MIBO TRADE promptly confirms the method and the time frame for execution, without preventing compliance with the GDPR time limits. Standard assistance and the remedying of non-conformities attributable to MIBO TRADE are included. Additional work, which does not represent obligations already assumed, may be charged only on the basis of an estimate accepted in advance; negotiating the cost does not suspend urgent measures or legal rights.

4.3. If a law of the European Union or of Romania obliges MIBO TRADE to process the Firm's Data otherwise, for example at the request of an authority, MIBO TRADE informs the Firm in advance, unless the law prohibits such notice.

4.4. MIBO TRADE immediately informs the Firm if it considers that an instruction infringes data protection law and suspends execution of the contested part until it is clarified or modified. Mere reconfirmation in writing by the Firm does not oblige MIBO TRADE to carry out an unlawful instruction. The parties cooperate towards a lawful solution; if this is not possible, only the affected processing or, if necessary, the Contract may be terminated, with the export and deletion provided here.

4.5. The Firm is responsible for the lawfulness of its instructions.

5. What the Firm does

5.1. Legal basis. The Firm ensures that it has a legal basis for each processing operation it carries out through the Platform (Article 6 GDPR and, for special categories of data, Article 9 GDPR) and that the data has been obtained lawfully, including the data about guests received from clients.

5.2. Information. The Firm ensures that persons are informed in accordance with Articles 13 and 14 GDPR, including the guests whose data it receives from the client and the Firm's Staff. It may use the client as an intermediary for the actual delivery of the notice, but remains responsible and keeps the evidence. For data

received indirectly, the information is provided within at most one month and, if it occurs earlier, at the first contact or the first disclosure. An exception to informing applies only after a documented assessment. The Cateruno templates must be completed and adopted by the Firm before use.

5.3. Only the necessary data. The Firm enters only the data it needs and does not upload copies of identity documents. In general fields (messages in the form and in the portal, notes, the seating plan, the reasons and notes of the Firm's Staff, files for import), no data is written about the health of identifiable persons, including about the author of the message, even without a name, nor any other special categories of data; a person's medical requirements go only through the flow in 7.2. The CNP is filled in only under the conditions in 7.4.

5.4. Access. The Firm keeps roles up to date, immediately removes from the team the people who leave, asks colleagues for strong passwords and two-step verification, keeps the personal links of clients and of the Firm's Staff confidential, approves for the page of a person in the team only that person's phones and immediately replaces a link that has reached someone else (article 7.7 of the Terms).

5.5. Requests from persons. The Firm responds to requests from clients, guests and the Firm's Staff (access, rectification, erasure, restriction, objection, portability), with the Platform's features and with the help in chapter 11.

5.6. Retention. The Firm determines how long it keeps the data and complies with its retention obligations, for example for contracts and for accounting documents (article 8.8 of the Terms). The periods that the Platform applies by default, as the Firm's instructions, are in Annex E; the Firm may shorten them and may extend them only where Annex E allows. Before deletion, the Firm exports what it must keep (chapter 15).

5.7. Impact assessment. The Firm documents before activation whether the processing requires an impact assessment, in accordance with Article 35 GDPR and ANSPDCP Decision no. 174/2018. The ordinary scheduling of the Firm's Staff, without assessment of persons, without special data, without monitoring and on a verified limited scale, does not in itself demonstrate a high risk. A report used to assess reliability or for repeated selection for work requires a new analysis before activation, with regard to profiling, the effects on income, the vulnerability of workers and the scale of use. The absence of solely automated decisions does not exclude an impact assessment. MIBO TRADE provides the technical documentation and an analysis template; the Firm takes responsibility for the conclusion adapted to its activity.

5.8. Content. What the Firm sends through the Platform (quotes, contracts, proforma invoices, messages, e-mail reminders) and the pre-written messages it sends from its phone (WhatsApp, SMS) are the Firm's content. The Firm is responsible for it and for the right to write to clients and to the Firm's Staff through these channels.

6. Confidentiality and MIBO TRADE's people

6.1. The Firm's Data can be seen only by MIBO TRADE's people who need it for a specific task (help requested by the Firm, security, fixing an error, maintenance, a legal obligation) and only for as long as they need it for that task. On the date of this version, there is a single person: the administrator of MIBO TRADE, who is also the administrator of the Platform. MIBO TRADE updates this information when it grants access to other people.

6.2. Every person with access is bound to keep confidentiality, by contract or by law, also after they no longer work for MIBO TRADE.

6.3. From within the Platform, the administrator of the Platform does not see the firms' data: enquiries, clients, events, quotes, contracts, payments and the Firm's Staff are seen only from the firms' accounts. In their administration area, which requires two-step verification, the administrator sees the access requests, the e-mail delivery status (the recipient's address, the type of message and the status), the Platform's error reports and the counts without names in 3.4. Direct technical access to the database is used only for the tasks in 6.1.

6.4. AI development assistants use synthetic or anonymised data and separate test environments by default. Access to real production data, including through screenshots, the administrator's browser, logs or files, is allowed only if necessary for a documented task, on the Firm's instruction and after the requirements for sub-processing and transfers are met. The administrator's technical approval does not replace these conditions. Automated database tests are run on a copy built from the same migrations, without the firms' data, and real client data is not used in conversations with the Lovable assistant. The Lovable assistant reads the production database only after approval by the administrator, given for each read.

6.5. The sub-processors' people access the data under the rules of their agreements (Annex C).

7. Data requiring extra care

7.1. Special requirements and allergies. The client portal asks for special requirements as a number of portions per category (vegetarian, Lenten or vegan, gluten-free and free from each of the 14 allergens in Regulation (EU) No 1169/2011), without the guests' names. The number of portions is not automatically anonymous: a requirement can identify the person even without a name, through context, through the table or at a small event, and the allergy or medical diet of an identifiable person is data concerning health, a special category under Article 9 GDPR. A culinary preference, for example the vegetarian menu, does not by itself prove a medical condition; the classification depends on the context.

7.2. The "Sensitive dietary requirements" flow. When the Firm needs the medical requirement of an identifiable person for serving, it processes it only through this separate flow, on the basis of the explicit, specific and demonstrable consent of the person or of their legal representative (Article 6(1)(a) and Article 9(2)(a) GDPR). The person receives a personal link, reads the notice and gives consent through separate, unticked boxes; the general statement of the client or of the organiser does not replace the guest's consent. For a child under 14, the parent or legal representative first states who they are and in what capacity, and the Firm verifies their representation before the Platform asks for the health information; for a child aged 14–17, the child's consent and the parent's approval are required, each through their own link and contact. The information reaches, as a minimal instruction, only the roles chosen for preparation and serving; the waiter called to the event sees it on their page only from 3 days before the event until the end of the last day of the event. It does not go into messages, e-mails, exports, reports, logs or AI requests. The requirement and the serving instruction are deleted immediately on withdrawal of consent and, otherwise, when no longer necessary, at the latest 30 days after the event. Separately, visible only to the Owner, the minimum evidence of consent remains, without the medical detail, for at most 3 years from the closing of the requirement. Limited retention for a specific dispute is assessed separately in accordance with Article 9(2)(f); it does not justify the preventive archiving of all allergies. An unsolicited message with health data, received in other fields, is not forwarded: access to it is restricted, and information without a legal basis is promptly removed.

7.3. Children are recorded by default only as a number of portions. Names on the seating plan or on name cards may nevertheless identify a minor; in that case, minimisation and appropriate information apply. The date of birth, the CNP or medical data of children are not requested; a strictly necessary named medical need goes only through the flow in 7.2, with verification of the person exercising legal representation.

7.4. The CNP is not mandatory for the ordinary invoice to a consumer and is not collected for the contract or for general identification. The field is optional and separate; it is filled in only if the beneficiary makes an informed choice to be identified for tax purposes by CNP or an applicable rule requires it. The Firm documents the situation and the specific legal basis; the processing necessary for invoicing and for the reporting required by law is based on Article 6(1)(c), in conjunction with the applicable tax rules, not on a general obligation to collect the CNP. If the beneficiary is not identified for tax purposes, the code of 13 zeros is used under the conditions of Article 10^1(3) of Government Emergency Ordinance no. 120/2021, as amended by Law no. 88/2026. Use based on legitimate interest triggers all the safeguards of Article 4(2) of Law no. 190/2018, including the appointment of a DPO. The CNP is removed from the reusable record after the invoice has been issued and checked; it remains only in the documents whose retention is legally required.

7.5. History of the Firm's Staff. The Platform keeps, for each person in the team, the planned shifts and the responses to invitations, for organisation purposes, for at most 12 months from the shift concerned. This data is planning, not attendance: the Platform does not keep timekeeping, hours actually worked, recorded absences, the CNP or medical documents and does not infer from an invitation or a confirmation that the person worked, was absent or how many hours they worked. It does not calculate scores, does not make rankings and does not take automated decisions about people; declining an invitation is not an absence and is not used against the person. The "Event attendance" report is not offered, because the Platform has no data on actual attendance. A "Planned shifts and confirmations in the last 12 months" report, which states that it does not prove attendance, absence or time worked, may be activated later only after the legitimate interest analysis, verification of the need for an impact assessment and informing the people. A report on actual attendance or an assessment of the collaboration requires a new analysis before activation, including, for employees, verification of Article 5 of Law no. 190/2018; health data does not go into any assessment.

7.6. Internal notes. The notes about clients, the team notes on events and the notes about the Firm's Staff are only for the Firm and are not shown to clients or staff, apart from the instructions that the Firm sends to the chosen roles. The Firm does not write in them special categories of data or assessments that it could not justify to the person it writes about, who may request them at any time (Article 15 GDPR). When it sends a client's message to the team, the Firm keeps only what is necessary for preparation and serving, without names and unnecessary details, without reducing the precision of the dietary instruction; health information goes only through the flow in 7.2.

8. The electronic signature and its evidence

8.1. When a client signs from the link, MIBO TRADE keeps on behalf of the Firm, as evidence: the name written by the signatory, the e-mail address at which they received the signing code, the confirmation of the code (the code has 6 digits, expires in 10 minutes and is kept only as a fingerprint), the image of the signature drawn on the screen, the date and time of opening, of sending the code and of signing, the signatory's IP address and browser and the SHA-256 fingerprint of the document. They appear in the electronic signing report added to the signed PDF, which is sent to both parties (article 9.3 of the Terms). For a consumer, their express request to start the services before the withdrawal period expires and the withdrawal statement sent online (the name, the e-mail, the services, the text and the date of receipt) are also kept, as the case may be.

8.2. When the client accepts from the link a new date for the event or acknowledges a price adjustment, MIBO TRADE keeps the date and time, the IP address and the browser.

8.3. The signed document and its evidence are not overwritten. Corrections are recorded through subsequent documents linked to the original. Integrity protection does not prevent legally necessary deletion or restriction, including while the account is active, after verification of the Firm's instruction and of the retention obligations. The actual deletion and its reason are logged without reproducing the deleted content.

8.4. The IP address and the browser from signing are seen only by the Owner, the manager and sales, and those from the acceptance of a new date or of an adjustment only by the Owner.

8.5. The Firm chooses the appropriate signing method and determines the retention period of the contract and of the evidence, on the basis of the legal obligations and the evidentiary need. MIBO TRADE keeps them only in accordance with the instructions and the duration of this agreement and includes them in the export. Account Closure does not reduce the Firm's archiving obligations; additional archiving at MIBO TRADE requires an instruction and conditions agreed before deletion.

9. Sub-processors

9.1. The Firm gives general written authorisation for the sub-processors identified in Annex C on the date of acceptance. The list shows the entity, the service, the data, the countries and the transfer mechanism, including the relevant chain of sub-processing. The updated list is published at cateruno.ro/furnizori. A

provider not yet identified cannot receive personal data; a feature that would use it remains switched off until Annex C is completed and the procedure in 9.3–9.5 is carried out.

9.2. MIBO TRADE verifies the guarantees of each sub-processor and contractually imposes on it data protection obligations equivalent to those applicable to the delegated activity, including security, confidentiality, assistance, incidents, audit, transfers and deletion. Standard terms do not remove the obligations of Article 28 GDPR. Procedural differences are acceptable only if they allow MIBO TRADE to comply effectively with this agreement; material inconsistencies are remedied before data is transmitted, or another solution is chosen.

9.3. MIBO TRADE actively notifies, by e-mail to the Owner, the addition or replacement of a sub-processor at least 30 days before it accesses the data. The notice states the activity, the data, the countries and the safeguards. If a genuine emergency does not allow this period, MIBO TRADE requests specific authorisation before transmission or temporarily suspends the affected processing; mere notice after the change does not replace the right to object.

9.4. For the providers' chain of sub-processing, MIBO TRADE obtains the necessary information and notices, assesses them and informs the Firm before the new recipient is used. Publishing or annually updating a list is not, on its own, sufficient. If the provider's mechanism does not allow compliance with this procedure, MIBO TRADE remedies the situation contractually or does not transmit data through the affected service.

9.5. The Firm may raise reasoned objections concerning data protection within 14 days of the complete notice. The parties seek an appropriate alternative before the contested processing begins. If they do not find one, the Firm may terminate the affected service without penalties, with export and a proportional refund of the amounts paid for the period not provided. This commercial solution does not exclude the damages or remedies provided by law for an attributable breach.

9.6. MIBO TRADE is liable to the Firm for its sub-processors as for its own acts, within the limits in chapter 14.

10. Transfers outside the European Economic Area

10.1. The Platform's database and file storage are in the Europe (European Union) region of Lovable Cloud; the database settings show the location "Europe (Ireland)". Hosting in the EU does not exclude transfers through remote access, support, e-mail, logs or AI: the Platform's e-mails are stored with the e-mail provider in the USA, and requests to the AI model may be processed outside the EEA. The transfers are described in Annex D.

10.2. Transfers are made only under the conditions of Chapter V GDPR: an adequacy decision applicable to the recipient and the processing, or appropriate safeguards, including standard contractual clauses from Decision (EU) 2021/914, with the module that matches the real roles. For the DPF, the active certification and the coverage of the transfer are verified; for the SCC, the law and practices of the country, the circumstances of the transfer and the necessary supplementary measures are assessed. The mere signing of the SCC or encryption in transit is not sufficient verification. The transfer is suspended when the safeguards are no longer effective.

10.3. A new transfer follows the procedure in 9.3–9.5.

10.4. On request, MIBO TRADE sends the Firm a copy of the safeguards, without confidential commercial information.

11. Help for the Firm

11.1. MIBO TRADE provides assistance with access, rectification, erasure, restriction and export, through the Platform's features or through a documented manual procedure. It confirms the Firm's request within two working days and provides the assistance, as a rule, within at most 10 working days, faster when the legal time limit or urgency requires it. The lack of a feature in the interface does not remove the assistance owed.

11.2. Requests from data subjects received directly are forwarded to the Firm without undue delay, as a rule within two working days. MIBO TRADE informs the person about the forwarding, keeps the evidence and does not decide the merits of the request concerning the Firm's Data without an instruction, except for its own legal obligations.

11.3. MIBO TRADE helps the Firm, with the information it has, to fulfil its obligations concerning security, Incidents, impact assessments and prior consultation of the National Supervisory Authority for Personal Data Processing (ANSPDCP) (Articles 32–36 GDPR).

11.4. Standard assistance is included, in accordance with article 4.2. An additional cost, accepted in advance, cannot condition urgent measures, the remedying of MIBO TRADE's own breach or the effective exercise of the persons' rights.

11.5. MIBO TRADE keeps a record of the processing activities it carries out for firms (Article 30(2) GDPR) and a register of Incidents and makes them available to the ANSPDCP on request.

12. Incidents

12.1. MIBO TRADE notifies the Firm without undue delay after becoming aware of a breach of the security of the Firm's Data and, contractually, within at most 24 hours of that moment. The 24-hour cap is a contractual obligation of MIBO TRADE; the legal obligation remains notification without undue delay. The initial notification may be incomplete and is updated successively. The conclusion of the investigation, the provider's formal confirmation or the establishment of fault is not awaited.

12.2. The notice goes to the Owner's e-mail and to the contact address for data, if the Firm has given one, and states, as far as is known at that moment: what happened; which categories and approximately how many persons and records are affected; the likely consequences; what MIBO TRADE has done and proposes; whom the Firm can contact. What is not yet known follows in phases, without undue delay (Article 33(3) and (4) GDPR). The Firm may report an Incident to MIBO TRADE at office@cateruno.ro.

12.3. MIBO TRADE immediately takes reasonable measures to stop the Incident and limit its effects, including temporarily stopping a link or a feature (article 18.2 of the Terms), preserves the evidence and records the Incident in its register.

12.4. The Firm assesses the risk in a documented way. It notifies the ANSPDCP without undue delay and, where feasible, within at most 72 hours of becoming aware, unless a risk to the rights of persons is unlikely. Any delay is reasoned. When a high risk is likely, it informs the persons without undue delay, subject to the exceptions in Article 34 GDPR. MIBO TRADE provides assistance and does not notify on behalf of the Firm without an instruction, except for its own legal obligation.

12.5. The notice of an Incident does not mean that MIBO TRADE admits any fault.

13. Information and audit

13.1. MIBO TRADE makes available to the Firm the information necessary to demonstrate that it complies with Article 28 GDPR: this agreement, the annexes, the list of sub-processors and, as far as the providers allow, their reports or certifications (Article 28(3)(h) GDPR).

13.2. MIBO TRADE answers reasonable questionnaires within at most 30 days, or sooner when there is an incident, a justified suspicion of non-compliance or a request from the authority. Routine checks are coordinated to avoid unnecessary repetition, without limiting the rights provided by Article 28 GDPR.

13.3. MIBO TRADE allows and supports audits and inspections by the Firm or by the mandated auditor. For routine checks, a notice period of 15 working days and a proportionate scope are proposed; incidents, justified suspicions and requests from the authority allow shorter periods. The parties first use documentary evidence if it is sufficient, but this does not exclude a necessary inspection. Duration and frequency depend on the risk, without a rigid cap. The auditor respects the confidentiality, security and data protection of other customers;

redactions or controlled access may be used, without concealing relevant evidence. The Firm bears its ordinary costs; MIBO TRADE bears the remediation and the reasonable costs of the verification required by a material non-compliance attributable to it. The conditions do not limit the powers of the ANSPDCP.

13.4. The Firm gives MIBO TRADE a copy of the report. Real non-conformities are corrected within agreed time frames.

14. Liability

14.1. Each party is liable for its own breaches of this agreement and of the GDPR.

14.2. Any compensation between the parties concerns proven and attributable damage, under the law, with due regard to causation, the duty to mitigate the damage and the right of defence. Administrative fines or the sanctioned party's own liability are not automatically transferred. Any recourse for amounts paid is analysed according to the applicable mandatory rules and the conduct of each party.

14.3. The contractual limits in chapter 17 of the Terms apply only to the relationship between the parties and only to the extent permitted by law. They do not limit the rights of data subjects, the powers of the authority, the mandatory liability provided by the GDPR or MIBO TRADE's obligation to answer for the performance of the sub-processors' obligations in accordance with Article 28(4). The recourse provided by Article 82(5) remains governed by that article.

14.4. The limits in 14.3 do not apply to damage caused intentionally or through gross negligence, nor in other cases in which the law does not allow limitation (article 17.4 of the Terms; Article 1355 of the Romanian Civil Code).

14.5. Towards data subjects, the parties are liable under Article 82 GDPR, and the limits between them cannot be invoked against data subjects. The party that has paid more than its share may claim the difference from the other, according to each one's share of fault (Article 82(5) GDPR).

14.6. The party that receives a claim notifies the other without delay and allows it reasonable participation in the defence. Cooperation does not prevent legal notifications, communication with the authority, the exercise of the persons' rights or urgent measures. A settlement that creates obligations for the other party requires that party's consent.

15. Export and deletion

15.1. Account Closure takes place in the cases in article 19.3 of the Terms: when the Owner confirms it in Settings › Delete account, at the end of Early Access or of the Free Trial without a chosen plan, and on any termination of the Contract (article 1.4 and chapter 18 of the Terms).

15.2. On termination, the Firm chooses between return by export and deletion of the data. In the ordinary closure flow, it has limited access for export for 30 days and may request earlier deletion, after confirming the export. The export comprises, in a usable format, the Firm's data and documents, including contracts, addenda, versions, evidence of acceptance and of signing, relevant correspondence, payment documents and, after their activation, debt files; electronic tax documents are exported in the form required by their regime, not only as a PDF for reading. Whatever the Platform's export feature does not include, MIBO TRADE makes available to the Owner, on request, in an archive prepared within the time limit in 11.1. Before deletion, MIBO TRADE informs the Owner of the export or migration period, the scheduled deletion date and the data that MIBO TRADE must keep under the law. If the Firm requests switching provider or migration under Regulation (EU) 2023/2854, the mandatory procedure and time limits in the Terms apply, including the retrieval period of at least 30 calendar days after the end of the transition period; deletion does not occur before they are completed. If the Firm requests only deletion, without switching provider, a transfer is not imposed on it as a precondition.

15.3. After the applicable export or retrieval period, MIBO TRADE deletes the active data, the files, the archive and the signed documents, subject to specific legal obligations. After Account Closure, access to the data is restricted to what is necessary for export, retrieval and deletion. Backups remain isolated, are not in current use and leave rotation within the cycle in Annex B; any restoration reapplies the list of deletions. The same discipline applies to sub-processors.

15.4. After deletion, only data required by law, strictly delimited and with restricted access, or irreversibly anonymised information may remain. The e-mail provider keeps the messages and logs sent through MIBO TRADE's account for 30 days from sending, according to its documentation for the plan used (Pro), and its backups for 7 days; early deletion of specific messages is requested from the provider. The closure of a Firm's account in Cateruno is not the closure of MIBO TRADE's account with the e-mail provider and does not start the 90-day period applicable to the closure of that account. MIBO TRADE's own invoices are kept separately, in its capacity as controller.

15.5. MIBO TRADE does not keep for the Firm the documents that the Firm must keep under accounting or tax legislation or under other laws; the Firm fulfils these obligations through export (article 8.8 of the Terms). At the Firm's request, MIBO TRADE confirms the deletion by e-mail.

15.6. Data deleted during the life of the account may remain for 30 days in the recovery archive (Settings › Archive), if the Firm does not request permanent deletion earlier and there is justification for this interval. Legally required deletion is not automatically postponed. For signed documents, the controlled procedure in article 8.3 applies; the integrity of the document does not equate to unlimited retention.

16. Amendments and final provisions

16.1. MIBO TRADE may change this agreement under the rules in chapter 4 of the Terms, without lowering the protection of the Firm's Data, for example when the law, the sub-processors or the Platform's features change. The activation of a feature marked "later" is announced to the Firm before the first processing, with the new version of the annexes; for a new sub-processor, 9.3–9.5 apply. If the Firm does not agree, it may close its account (article 4.3 of the Terms), with the export in 15.2.

16.2. The Platform keeps each acceptance of the Terms, and therefore of this agreement, with the version, the date and time, the person and the source (article 3.6 of the Terms). The agreement has its own version, separate from that of the Terms and of the information notices, and the accepted version remains available to the Firm.

16.3. Communications are made under chapter 21 of the Terms: to the Firm, at the Owners' addresses and, for Incidents, also at the contact address for data; to MIBO TRADE, at office@cateruno.ro.

16.4. The applicable law and the competent courts are those in article 22.6 of the Terms.

16.5. The unusual clauses that fall under Article 1203 of the Romanian Civil Code are highlighted in the Terms and are accepted expressly in writing, including electronically, through the separate mechanism provided there. Acceptance does not validate derogations from mandatory GDPR rules and cannot turn the audit conditions into a waiver of legal rights.

16.6. If a clause is void, the others remain valid, and the void clause is replaced as in article 22.4 of the Terms.

16.7. The Romanian version takes precedence over the English translation.

Version 2, dated 10 November 2026.

Annex A. Details of the processing

The categories below are processed only for the features actually activated, in accordance with the Firm's documented instructions and with the purposes and durations in the DPA. The description of a future feature does not authorise processing before the contractual, information and security conditions are met. The operations for which MIBO determines its own purposes are described separately in its privacy notice.

Table A.2 describes the features active on the date of this version; table A.3, the features marked “later”, which are activated only after the procedure in 16.1, together with their measures, providers and information notices.

A.1. Elements of the processing

Element	Description
Subject matter	Provision of the Platform for catering firms: enquiries, clients, the catalogue (including AI import), quotes, contracts and electronic signing, the client portal, events, payments and proforma invoices, the crew at events, production and printed materials, guests’ sensitive dietary requirements. The features in table A.3 come later.
Duration	For as long as the Firm has an account, plus the export, retrieval and deletion period in chapter 15.
Nature	Collection through the Platform’s forms and through the links for clients, guests and the Firm’s Staff; storage; organisation; display by role; calculations; generation of PDF documents; sending by e-mail; preparation of the messages that the Firm sends from its phone; electronic signing; reading of catalogue files with AI; backups; export; deletion.
The Firm’s purposes	Quoting, contracting, organising and invoicing events; communication with clients, guests and the Firm’s Staff; preparing and serving menus, including adapting them to dietary requirements; keeping records of payments and costs.
What MIBO TRADE does for them	The Platform’s features, security, the help requested, backups, fixing errors, export and deletion.
Instructions	Chapter 4: this agreement, the Terms, the use of the Platform by the Authorised Persons, the Firm’s settings (the roles, access, the features switched on, the retention periods chosen from Annex E) and the Owner’s written requests.
Location	The database and file storage: Lovable Cloud, Europe (European Union) region, at the location in 10.1. Backups: Annex B. Transfers and access from outside the EEA: Annex D.
Frequency	Continuous, for as long as the Firm uses the Platform.

A.2. Data subjects and data, for the active features

Data subjects	Data and limits	Where they appear and conditions
Enquirers and contact persons (enquiries)	The name and the necessary contact details; the characteristics of the event, the budget, the preferences and a minimised message; the data entered by the team when creating a personal link (the phone number and, optionally, the name and e-mail) and the source of the enquiry. The portion quantities needed are not automatically classified as anonymous; identifiable medical data is excluded from the general form and handled only in the flow in 7.2.	The Firm’s form (fixed link and QR code) and the personal links, which do not display the person’s data and expire after 30 days; Enquiries; quoting. The confirmation by e-mail is neutral: it does not reproduce the content of the enquiry and does not sign the person up for commercial messages.
Visitors to the enquiry form and to the other pages opened by link	The IP address and the technical metadata strictly necessary for display and for preventing abuse, including before the form is submitted. For limiting the enquiries sent through the form, the IP address is kept for at most 48 hours; for the technical logs of hosting and of the network, the actual duration is in Annex E.	Hosting, the connection, limiting requests and security. The role of each operation and the infrastructure are documented; MIBO TRADE’s own processing is explained separately, in its privacy notice.
The Firm’s Clients who are natural persons	Name, e-mail, phone, address, language; CNP, optional (7.4); the Firm’s internal notes.	The client record; enquiries, quotes, contracts, addenda, proforma invoices and e-mails to the client. The CNP is seen only by the Owner and the manager; the notes, by the Owner, the manager and sales.

Data subjects	Data and limits	Where they appear and conditions
Representatives and contact persons of client firms	Name, position, e-mail, phone; the public data of the client firm from the ANAF register, fetched by CUI; the uploaded electronic signature agreement, with the representative's name and signature.	The client record; the documents.
Clients, for the quote and signing	The first and last opening of the quote link and the number of openings; the response (acceptance, refusal, request for a new quote, the client's note); the evidence of signing and of acceptances (chapter 8); for consumers, the request to start before the withdrawal period expires and the withdrawal sent online.	The pages behind the links; the quote page and the contract page; the History.
Clients, for payments	Instalments, payments (amount, date, method, document), overdue amounts, the amount in the client's favour; proforma invoices and payment reminders.	The event's Payments tab; Money › Payments and Money › Proforma invoices; the client portal; e-mails.
Invoices through the Firm's Oblio or SmartBill account and e-Factura: invoiced clients	The client's billing data, including the CNP under the conditions in 7.4.	The account and the API key are the Firm's (2.4); only after the Firm connects its account.
Clients, in the client portal	The final guest count and change requests, special requirements as a number of portions, messages with the Firm, tastings, the seating plan, proforma invoices to download.	The client portal; the Client portal tab on the event page.
Guests at events	Portion totals; name or identifier, group and table, if strictly necessary; the names on the name cards; may include minors; health or other special categories only through the flow in 7.2.	The seating plan in the portal; printed materials (name cards); kitchen sheets, without names.
Guests and their representatives, in the "Sensitive dietary requirements" flow	The person, the dietary requirement that reveals health and the serving instruction; the explicit consent, with the version of the accepted text; for a child, the representative, their capacity and the verification; for ages 14–17, the child's consent and the parent's approval; the minimum evidence of consent.	The dedicated flow (7.2), with personal links; the instruction reaches only the chosen roles; outside messages, e-mails, exports, reports, logs and AI requests.
The Firm's Staff: waiters, bartenders, chefs, assistants, hosts, drivers	Name, phone, optional e-mail, roles, the form of collaboration (employee, day labourer, self-employed (PFA)), the rate per hour or per shift, active or inactive status; planned shifts (the role, the planned arrival and departure time), the responses to invitations and the optional reason; the days on which the person cannot work, with an optional short note; the phones approved for the personal page; reminders. No timekeeping, hours actually worked, recorded absences, CNP, medical documents or medical reasons.	Team; the person's page, from their personal link; e-mails; WhatsApp messages sent from the Firm's phone. The record, with the rate, is seen only by the Owner, the manager and the head waiter. The shift history is not an attendance report (7.5).
Authorised Persons, in the Firm's account	Name, e-mail, phone (if filled in), the role and access tiers, the actions in the History and in the audit log, notifications; the name and phone of the contact person and the e-mail of the sender are shown to the client.	Settings › Team; the History; the client portal; e-mails to the client.
The Firm's suppliers and their contact persons	Name, CUI, contact person, phone, e-mail, notes; the "To order" lists, sent to the supplier from the Firm's phone.	The catalogue (ingredients and suppliers); "To order".

Data subjects	Data and limits	Where they appear and conditions
Persons who may appear in the files imported with AI	The catalogue content of the file (dishes, descriptions, prices, allergens) and the technical metadata of the request. The flow prohibits data about persons; a name left in a file by mistake remains personal data.	Catalogue, AI import (3.5), only for the Owner and the manager; the file is deleted from the Platform immediately after reading.
Recipients of e-mails	The e-mail address, the type of message, the date, the delivery status (sent, delivered, rejected, reported as spam), the content and the attachments.	The Platform's e-mails.
All of the above, technically	The Platform's error reports (without the URL parameters, kept for 30 days), the rows in the History and in the audit log, the technical logs of hosting.	The database; hosting.

A.3. Features marked "later"

Feature and data subjects	Data and limits	Use and activation conditions
Formal notices (later): clients, representatives and recipients of correspondence about debts	The relevant identification, the formal notice, the amounts and interest, the postal or bailiff's evidence, including the data of the person receiving, and the necessary factual notes. No data unrelated to the dispute.	Overdue and Formal notices; the debt file, with a review date and reasoned additional retention (Annex E).
Equipment (later): clients and persons involved in recording damage	The written report, the description, the relevant photos, the observations, the proposed amount, the author or the signatory, where applicable. Incidental capture of persons and of unnecessary documents is avoided.	Logistics, damage recording and Payments; limited access and retention according to purpose and evidence.
Partners (later): natural persons or self-employed persons (PFA), the partners' contact persons and representatives	Professional identification and contact data, the necessary capacity or mandate, the arrangement with the Firm and the responses about availability; data relating exclusively to the company is not automatically classified as personal data.	Catalogue › Partners and the event page; organising and proving the collaboration.
Vehicles (later): the designated staff and the recipients of messages	The designated driver, the planned or actual departure and return times, marked separately; the minimised text of the messages, the recipients, the date and the delivery status. No GPS or tracking of movements.	Logistics and Team › Messages; scheduling and service communications, without medical reasons or distribution to recipients without need.
The voice assistant (later): its users and the persons mentioned in commands	The text of the command and the transcription, with a history of at most 30 days; the recording started by the user, of at most 30 seconds, processed temporarily for transcription, without persistent archiving in Cateruno after completion, if this is verified; the strictly necessary catalogue content and the indispensable technical metadata. Health data and other unnecessary personal data: prohibited in commands.	The assistant and its history. MIBO TRADE is the Firm's processor, and the AI provider is a sub-processor authorised under chapter 9. The provider's identity, the routing, the countries, its own retention, deletion and non-training are completed from contracts and settings verified before activation. The minimal log of the approved change has its own purpose and period.
Contract templates imported with AI (later): the persons named in them	The minimised text of the template, preferably without identifiable persons. Names and professional data left in are personal data; CNPs, signatures, medical data, personal bank details and case details without necessity are removed.	Settings › Contracts, the division into chapters; review before transmission to the AI provider, without using the external service for the first anonymisation of the raw text.

Feature and data subjects	Data and limits	Use and activation conditions
AI menu proposal (later): enquirers	Only the necessary structured fields, after minimisation: the type and month of the event, the number of guests, the budget and the culinary preferences. The name, the contact details and the free-text message are excluded; the special portion quantities needed are transmitted only if they do not reveal the health of identifiable persons.	Activation only after verification of the flow (3.6) and update of the annexes and of the notice for clients.
SMS messages sent by the Platform (later): recipients	The phone number and the text of the message.	After the provider is chosen and Annexes C and D are completed.
Card payment (later): the Firm's Clients who pay online	The reference, the amount, the currency and the contact details necessary for the transaction; the payment confirmations (the identifier, the amount, the status). Full card data does not reach MIBO TRADE.	Article 2.6; the Firm's payment service provider is not a sub-processor of MIBO TRADE.
Reading suppliers' invoices and receipts (later)	The data on the uploaded documents, where names of persons may also appear.	Ingredient prices; activation after verification of the AI flow (3.6).
The online menu, the embedded module and the Firm's website (later): visitors	The technical connection data on display and the data sent through the enquiry; storage in the browser only for as long as strictly necessary for the selection.	Activation after analysis of the roles of each flow, of storage on the device and of the notice next to the module.
Timekeeping and any report on actual attendance (later)	Not collected until activation.	New analysis before activation (7.5).

Special categories of data: health and, possibly, information revealing religious beliefs through named dietary requirements, only under the conditions of articles 7.1–7.2. CNP: article 7.4. Data about children: aggregated totals and, exceptionally, strictly necessary named data in accordance with articles 7.2 and 7.3. The static image of the signature is not automatically special biometric data; if technical processing for unique identification is introduced, Article 4(14) and Article 9 GDPR are reassessed. The voice, for the voice assistant (later), is personal data; transcription without identification of the speaker is not, in itself, biometric identification.

Annex B. Technical and organisational measures

The annex describes the measures existing on the date of this version, as they result from the Platform's code, from its automated tests and from the providers' documentation. The contractual obligation remains the implementation of the appropriate measures in Article 32 GDPR, including confidentiality, integrity, availability, resilience, restoration and periodic verification.

Area	Measure
Separation of firms	Each table with a firm's data carries the firm's code, and the database (PostgreSQL, with row-level access rules) lets a user read and write only in the firms of which they are an active member. Links to another firm's rows (events, quotes, rooms, suppliers, ingredients, prices, portal, files) are refused by the database. The separation is verified by automated database tests.

Area	Measure
Roles and minimum necessary access	Seven roles: owner, manager, sales, kitchen, head waiter, staff, accountant. Costs, margins and profit are in separate tables, read only by the roles that are allowed to. The kitchen and the staff do not read prices, costs, quotes, contracts, payments or client records; the head waiter reads events as the kitchen does and does not read quotes, contracts, payments, costs or catalogue prices. The Accountant has tiered access, by default “Payments received only”, and does not see the CNP, the notes about clients, the signatures or the signing agreements. The records of the Firm’s Staff, with the rate, are seen only by the owner, the manager and the head waiter. A member’s role and access change only through functions that leave a trace in the log, and the Owner is notified when a manager changes the team.
Two-step verification	Mandatory for the administrator of the Platform from the first login and for Owners before the first sensitive step (Terms, 7.1): sending a contract or an addendum, issuing a proforma invoice, recording a payment, exporting data, inviting a colleague and opening the dietary requirements or a client’s CNP, with the code from the authenticator app and 10 backup codes kept only as fingerprints. Until the first sensitive step, the app recommends it to the Owner at every login; once switched on, Owners cannot switch it off. Also required for data export, for managing the team and roles and for the payments or costs written by the accountant. The Platform’s administration area and the access request data require a two-step session.
Accounts	Accounts are created only from personal, single-use access links, valid for 7 days and kept only as a fingerprint; in Early Access there is no open sign-up. Passwords are not kept in the Platform’s tables; they are managed by the Lovable Cloud authentication service, which, according to Lovable’s documentation, keeps them only as a fingerprint (hash).
Limiting attempts	Logging in, codes by e-mail, access links, signing codes, the enquiry form and error reports have limits per minute, per hour or per day. What is kept for counting (the IP address or a fingerprint of it) is deleted after at most one day; for the enquiry form, after at most 48 hours.
Personal links	The quote, the contract to be signed, the client portal, the personal form link, the page of the person in the team and the links for dietary requirements open from personal links, with a random code of at least 128 bits. The codes of quotes and of the links for dietary requirements are kept only as a fingerprint; the others are in tables that only the server reads, except for the form links, which are also seen by the Firm’s members with access to enquiries. The page shows only the document or event of the link; visitors without an account do not read the tables directly, and every action goes through the server. The pages of the form and of the person in the team are not indexed by search engines and do not pass on the page address.
The Firm’s Staff page	The personal link opens the page only on registered phones: the first phone, on first opening, and any other only after the Firm’s approval. A phone not used for 180 days is closed, and the link can be replaced at any time. The page shows only the person’s shifts from yesterday onwards, without client, prices or colleagues.
Signing and document integrity	The signing code has 6 digits, expires in 10 minutes, is kept only as a fingerprint, can be requested at most once per minute and allows at most 5 attempts; the signature is bound to the SHA-256 fingerprint of the exact version of the document. Signed documents are not overwritten; lawful deletion or restriction is done through the controlled procedure in article 8.3. SHA-256 verifies integrity; it does not by itself prove identity or a qualified time stamp.
Transport	The Platform, the links in e-mails and the server’s connections to the database, to the e-mail service and to the AI service use HTTPS addresses (TLS-encrypted connections). The Platform’s pages cannot be framed in other sites.
Storage	The database and the files are in Lovable Cloud, Europe (European Union) region, at the location in 10.1. Lovable states that stored data is encrypted with AES-256, with keys managed by the service; the project’s secrets (the service keys) are encrypted separately, with per-workspace keys in Google Cloud KMS. The public documentation does not state separately, for the database, the files and the backups, who controls the keys.
Files	Uploaded logos, PDFs, signatures and agreements are kept in a private file storage, divided by firm, and are downloaded through temporary links (5 minutes for contracts and agreements, one hour for logos and photos). Contracts and agreements are read and written only through the server. Files for AI import are kept in a separate storage, to which only the owner and the manager of the firm have access, and are deleted immediately after reading.

Area	Measure
Backups	The database: one copy per day, made by Lovable Cloud, with a history of approximately 14 days for restoration, according to the provider's public documentation; files are not included in these copies. Lovable's DPA states that deleted data may remain in backups "for a limited period", without a maximum period, and the documentation does not state separately where the copies are kept (Lovable states that data remains by default in the chosen region). A restoration can be performed only by MIBO TRADE's administrator and involves reapplying the deletions made after the date of the copy, so that expired data does not re-enter current use.
Automatic retention	Daily scheduled jobs delete: lost enquiries, after the period chosen by the Firm; items in the Archive, after 30 days; inactive people in the team, 12 months after their last shift; the shift history, after 12 months; sensitive dietary requirements, 30 days after the event, and their evidence, after at most 3 years; error reports, after 30 days; counting traces, after at most 48 hours.
The log	Important actions (sending quotes, signatures, payments and their deletion with a reason, changes of role and access, exports, permanent deletions from the Archive, failed AI imports) leave a row with the author and the time in the History or in the audit log. The audit log is seen by the Owner and the manager. The rows in the History and those in the audit log do not contain IP addresses; the signatory's IP address remains only in the evidence of signing.
Export	Only the Owner, the manager and the accountant export the data, with two-step verification, and the export starts only after its row in the log has been written. The export in Settings includes the firm's core data (the firm, the team members, the invitations, the venues and rooms, the fixed costs and the audit log); for the rest of the data, 15.2 applies.
Minimisation	The CNP is optional, separate from the client record, visible only to the Owner and the manager and removed from contracts. Special requirements are asked for as a number of portions, not by name; named medical ones go only through the flow in 7.2. The personal form link does not display the person's data. Error reports keep the page without the URL parameters, the browser only for those logged in, and are deleted after 30 days. The Platform's code does not include third-party analytics or advertising tools.
AI	Catalogue import: only the owner and the manager, only in the plans that have the feature, at most one import every 10 seconds, JPG, PNG, WebP or PDF files of at most 8 MB. The server sends the file to Lovable's AI service (Annex C), with the instruction to extract only the dishes, and receives a table of proposals; nothing is saved in the catalogue without the user's review and confirmation, and the results are checked by a person. Lovable's "AI app context" setting is switched off, so the content of requests is not captured through this feature; Lovable nevertheless records a technical summary of each request. The app asks, on each call, that the response not be stored by the service; the effect of this option at Lovable and at the model provider is not confirmed, and their retention is the one in Annex C. Clients' messages, free-text fields and health data do not reach AI.
Data accuracy	When a read from the database fails, the Platform stops the sending, signing or saving, instead of using empty data. The client responds only to the version of the quote they see.
Secrets	The service keys (server access to the database, e-mail, AI, verification of delivery notifications) are kept only on the server, never in the browser; the browser receives only the public key of the database, and the row-level access rules apply to any request made with it. When the Oblio or SmartBill integrations are activated, the firms' keys are kept encrypted and do not reach the browser.
Access by MIBO TRADE and by providers	Privileged access is limited, justified and authorised; the administrator of the Platform does not see the firms' data from within the app (6.3). Development AI uses synthetic data by default; any access to production through the browser, screenshots or the database follows article 6.4 and the authorised chain of providers; the administrator's technical approval does not replace the GDPR conditions. On the Business plan, Lovable does not document a log of each direct read from the database (the workspace audit log, with the queries executed, is documented for the Enterprise plan); therefore MIBO TRADE records each direct access to the production database in an internal register: the date, the person, the purpose and what was read. For support, Lovable states that it accesses data only when necessary and approved by the customer, limited by roles, with multi-factor authentication and centralised logging.
MIBO TRADE's accounts with providers	Two-step verification on the Lovable, GitHub, Resend, Romarg and Google Workspace accounts.

Area	Measure
Checks	Over 140 automated database tests (separation of firms, what each role sees, the accountant, files, public links, retention and deletion), run on a copy of the database when the rules change. The security review of the access rules, the public pages and the server code is carried out before the first firms are activated and after important changes; the date and the result are kept by MIBO TRADE.
E-mails	Sent from the app.cateruno.ro subdomain, authenticated with SPF and DKIM, with a DMARC policy; the sending domain is in the provider's Ireland region (eu-west-1), but the provider stores the data in the USA (Annex D). Clients' replies go directly to the address of the person in the Firm who sent the message. The delivery status comes only through signed notifications from the provider, verified by the server. The logo in the e-mail is loaded through a link that gives no access to documents.

Annex C. Sub-processors

The list shows the sub-processors active on the date of this version, authorised in accordance with chapter 9, with the entity, the capacity (direct or in the chain), the service, the data, the location and the agreement. The updated list is published at cateruno.ro/furnizori. The providers in table C.2 do not receive data before activation and the procedure in 9.3–9.5.

C.1. Active sub-processors

Entity	What it does	What data it touches	Where the data is kept	Agreement and safeguards
Lovable Labs Incorporated, USA, direct	Hosting of the Platform and of the backend (Lovable Cloud: the database, authentication, file storage, server functions, backups) and the AI service through which the catalogue import is carried out; it is also the environment in which the app is built. Its chain, from the public list, is in table C.1.1.	All the Firm's Data, including the optional CNP (7.4) and the dietary requirements from the flow in 7.2; for AI, the import file, the response and the technical summary of the request.	The database and the files: Europe (European Union) region, at the location in 10.1. The countries from which Lovable and its sub-processors may access the data for support and administration are not published; access from outside the EEA is treated as possible (Annex D).	Lovable's public DPA (updated on 6 November 2025), which applies to the Business and Enterprise plans; Lovable's frequently asked questions state that the DPA is included in the Business plan and applies through the terms of service, without a separate signature. MIBO TRADE archives the signed version published by Lovable (Lovable_DPA_17Nov2025_Signed.pdf). SCC from Decision (EU) 2021/914, module 3, for MIBO TRADE as processor. Lovable undertakes not to use the customer's personal data to train models (section 10); its service data is governed by section 9. Lovable's list of sub-processors is updated at least annually, with objections within 20 working days. "AI app context" is switched off.

Entity	What it does	What data it touches	Where the data is kept	Agreement and safeguards
The AI model provider, in the chain, through Lovable: Microsoft Azure AI Foundry or OpenAI, depending on Lovable's route; Lovable lists both for AI (C.1.1), but does not publish the route of calls to this model on the Business plan	Reads the import file (photo or PDF of the menu) and returns the item proposals; the model used by the Platform is OpenAI GPT-6 Astra.	The content of the file (dishes, descriptions, prices, allergens) and the technical metadata of the request; the flow prohibits data about persons, without excluding a name left in by mistake.	The Netherlands, France, Germany or the USA, depending on the route; on the Business plan, processing in the EU is not guaranteed (EU inference is an Enterprise option).	Lovable's DPA: SCC for transfers without an adequacy decision (section 8.2); Lovable states contractual training and retention restrictions for AI providers. With "AI app context" switched off, Lovable does not keep the request and the response, but a summary of the call (the model, the time, the status, the cost). Retention at the model provider is not published for this flow; zero retention is documented only on the Enterprise plan.
Plus Five Five, Inc. (Resend), USA, direct	Sends the Platform's e-mails: quotes, contracts, signing codes, addenda, proforma invoices, reminders, invitations for the Firm's Staff, notifications, account e-mails.	The recipient's address, the content and the attachments (the PDFs), the metadata and the delivery logs.	Sending from the Ireland region (eu-west-1); storage in the USA, regardless of the sending region. Pro plan: messages and logs are kept for 30 days while the account is active; backups, 7 days; on the closure of MIBO TRADE's account with Resend, the remaining data is deleted within 90 days.	Resend's DPA (updated on 31 December 2025); SCC from Decision (EU) 2021/914, module 3. Resend states that it holds DPF certification, but MIBO TRADE relies on the SCC, which do not depend on it. Resend's new sub-processors are announced at least 14 days in advance. The closure of a Firm's account in Cateruno is not the closure of MIBO TRADE's account with Resend.
Google Ireland Limited, Ireland, direct (Google Workspace)	The office@cateruno.ro mailbox, when the Firm or a person writes to MIBO TRADE and puts the Firm's Data in the message (support, requests from persons, Incidents).	The data in the messages and in the attachments.	Google's data centres, in several countries.	Cloud Data Processing Addendum applicable to the Workspace account; for transfers to Google LLC, the EU–US adequacy decision for certified entities, otherwise SCC. CDPA accepted in the Workspace account console on 9 November 2026.
Cloudflare, in the chain, through Lovable	DNS, traffic routing and Cloudflare Workers, where the app's server functions run (TanStack Start apps are published on Workers, according to Lovable's documentation).	The traffic, the IP address and the request headers, and the content of the requests processed by the server functions.	Global network.	In Lovable's chain; Cloudflare's standard DPA names Cloudflare, Inc. as importer, but Lovable does not publish the entity contracted for the project.

C.1.1. Lovable's chain, from its public list

Lovable's public list of sub-processors (trust.lovable.dev/subprocessors), consulted on 9 November 2026. It gives the role and location of each provider, without linking it to the project and without the legal entity and the transfer mechanism of each; MIBO TRADE keeps a copy of the list as at the date of acceptance.

Provider	Role published by Lovable	Published location
Supabase	Databases and authentication	EU, by default
Google Cloud Platform	Infrastructure, applications, databases and keys (KMS)	The Netherlands (europe-west4)
Amazon Web Services	Infrastructure, storage and AI inference	London, for storage, cache and secrets; Oregon (USA), for Bedrock inference
Cloudflare	DNS, routing at the network edge and Workers	Global
ClickHouse and Altinity	Analytics of published apps and operation of the cluster	EU
Grafana	Logs and metrics	USA
Sentry	Performance monitoring	USA
Microsoft Azure AI Foundry	AI Gateway inference	The Netherlands, France, Germany, USA
OpenAI	AI interactions	USA

C.2. Later, before activation

Provider	What it will do	Condition
The SMS provider (to be chosen)	Sends the SMS reminders to the Firm's Staff: the phone number and the text of the message.	DPA, locations (preferably in the EU), retention, sub-processors and transfers completed; the procedure in 9.3–9.5.
The AI providers for the voice assistant, the menu proposal, the reading of invoices and the import of contract templates	Transcription and interpretation of commands; menu proposals; reading of documents.	The entity, the models, the countries, audio and text retention, the training prohibition and the transfer mechanism completed in Annexes C and D before activation (3.6).

C.3. Not sub-processors of MIBO TRADE for the Firm's Data

Service	Why
Oblio, SmartBill (for the Firm's invoices, from the beta launch, after the Firm connects its account)	The account and the API key are the Firm's. The role of the service is established according to the contract and the actual operation; the Firm concludes a DPA when the service processes on its behalf.
NETOPIA (later, after card payment is activated)	The payment service provider contracted by the Firm; it acts as an independent controller for the payment service's own purposes and its legal obligations (2.6). The entity is the one in the Firm's contract.
Stripe and SmartBill, for MIBO TRADE (from the Launch)	MIBO TRADE will collect the Subscriptions through Stripe and will issue its invoices to the Firm through SmartBill, with the Firm's billing data, as a controller (2.5).

Service	Why
WhatsApp and the phone's SMS app	The pre-written messages are sent from the Firm's phone and account; the Platform does not send or read WhatsApp or SMS messages.
The maps app, on the page of the person in the team	A link to Google Maps, with the venue address, opened only when the person taps it.
The Firm's calendar (later)	The calendar will read the calendar link that the Firm adds to its account.
ANAF	The Platform looks up the firms' public data by CUI and sends only the CUI and the date.
NBR	The Platform reads the day's exchange rate and does not send personal data.
Romarg SRL	Domain registration and DNS. It is not a sub-processor for the firms' content, which it does not receive; it may process the registrant's contact data and logs specific to its service.

Annex D. Transfers outside the EEA

Recipient	Country	Data	Safeguard
Lovable Labs Incorporated	USA	The Firm's Data, when needed for administration, support or the AI service.	SCC from Decision (EU) 2021/914, module 3, in Lovable's DPA; the transfer assessment and the necessary supplementary measures; the countries of access, as in Annex C.
The AI model provider, through Lovable	The countries in Annex C; they may be outside the EEA, including the USA.	The import file and the response.	The mechanism in Annex C.
Plus Five Five, Inc. (Resend)	USA	The e-mails, the recipients' addresses, the attachments, the logs.	SCC from Decision (EU) 2021/914, module 3, in Resend's DPA; the DPF certification stated by Resend is not the condition of the transfer.
Google LLC, through Google Ireland Limited	USA and other countries	The messages sent to office@cateruno.ro.	The EU–US adequacy decision for DPF-certified entities and the transfers covered, otherwise SCC and appropriate measures; the Workspace DPA, as in Annex C.
Cloudflare, through Lovable	Global network	The Platform's traffic, the IP address and the headers; where applicable, the requests processed by the server functions.	The entity, the service and the safeguards in Lovable's chain, as in Annex C.
Lovable's chain in the USA: Grafana, Sentry, Amazon Web Services (Bedrock inference), Microsoft Azure AI Foundry and OpenAI, as applicable	USA	Technical logs and metrics, which may contain the IP address; for AI, the import file and the response.	SCC in Lovable's DPA (section 8.2), in the chain; the DPF certification of the US entity, where applicable.

MIBO TRADE documents, for each flow, the country, the recipient, the transfer mechanism, the risk assessment and the necessary supplementary measures. The providers' reports are evidence to be analysed, not automatic substitutes for MIBO TRADE's own assessment. Encryption in transit does not exclude the provider's access to the decrypted content; minimisation, pseudonymisation, key control and access are verified. For AI, the training prohibition and retention must result from the applicable agreement. A transfer for which the safeguards are not completed in this annex does not take place.

Annex E. Data retention

The periods below are the Firm's default instructions for the Platform, apart from the periods expressly provided by law. They are internal policy periods, not periods imposed by the GDPR. A maximum period does not oblige the retention of data that is no longer necessary. Truly anonymised data may be used for statistics; removing the name or replacing it with a code is not, on its own, anonymisation.

The period starts from an objective and verifiable event. Automatic communications, the mere accessing of a page, a migration or an insignificant internal change do not restart the periods. Suspension of deletion is targeted: the necessary set, the legal reason, the person responsible, the date and the re-examination, at least every six months, are identified; once the reason ceases, deletion applies. The right to erasure is dealt with individually, without waiting for the period to expire. On restoration from backups, the register of deletions is reapplied. A person's access through the portal or through the personal link may end before the retention period; closing access and deleting data are different operations. Keeping contacts does not constitute permission for marketing.

E.1. Active features

Data	Period and starting point	Exceptions and application
Enquiry declined, withdrawn or closed, without a contract	6 months from closure; data that is no longer necessary is removed earlier.	The Firm may choose 12 months only for a real contracting cycle, documented and explained in the notice. Evidence of a specific complaint or claim is separated; the whole file is not kept automatically.
Enquiry without an answer, without active negotiation	6 months from the last substantive communication about the enquiry.	Opening the page, automatic e-mails and internal changes do not restart the period.
Real negotiation for a future event	While it is active and the data is necessary; review every 3 months.	12 months from the last substantive communication only if the real cycle justifies it; otherwise 6 months apply. The "open" status does not by itself suspend deletion.
The client's operational record after the last event (the reusable record, usual preferences, logistics messages, working copies)	12 months after the last event completed or cancelled.	Order or contract in progress: only the data necessary for that purpose, without automatic extension for the data of old events. 24 months only for documented recurring relationships, with information and a legitimate interest analysis; not activated for the whole client base.
Guest lists, table seating and name cards	Removal when the purpose of serving has ended; at most 30 days after the event.	Extracts needed for a specific complaint are kept separately; the client record period does not apply.
Sensitive dietary requirements and serving instructions	Removal when no longer necessary, at the latest 30 days after the event; immediately on withdrawal of consent.	Explicit consent does not allow unlimited retention. The medical detail is not archived unnecessarily.

Data	Period and starting point	Exceptions and application
The minimum evidence of consent for sensitive requirements; the verification of a child's representative	At most 3 years from the closing of the requirement or from the verification, respectively.	Separately, without the medical detail; the evidence is seen only by the Owner. Retention for a specific claim is reasoned. The verification is reused only for the same representative and the same client.
The operational record of an inactive person in the Firm's Staff	12 months after the last planned shift; with no shift, from being added to the list or from the last real discussion about collaboration.	A cancelled future shift counts from the date of cancellation. Late deactivation does not restart the period. An agreed future shift means ongoing collaboration.
History of planned shifts and of responses	At most 12 months from the shift concerned, if the seasonal need is documented.	Not actual attendance. A shorter period is chosen if it is sufficient; employee monitoring has special rules.
Optional notes and reasons of the Firm's Staff (unavailability, refusal)	As long as necessary for organisation, at the latest 30 days after the shift or period they refer to.	No health or other private details; impermissible information is removed promptly. Not used for scores or against those who refuse.
Contracts, addenda and their evidence (evidence of signing and of acceptances)	A separate schedule, by obligations and claims, including the effect of the applicable limitation period; the Firm sets the period (8.5).	Not deleted under the 12-month rule for the operational record; there is no universal rule of 3 years from the event. Signed documents are not deleted automatically.
Accounting registers and supporting documents (Article 25 of Law no. 82/1991)	5 years from 1 July of the year following the end of the financial year in which they were drawn up.	Kept by the Firm, through export (15.5). They do not automatically include logistics messages and all data about clients.
Employment, day labourer and payroll documents	The specific statutory periods, in a separate record, kept by the Firm outside the Platform.	The Team module is not timekeeping or an official register; the rule for inactive people does not affect these records.
The event's History and the audit log	The History, as long as the event; the audit log, until Account Closure.	Deleted together with the event and with the account data, respectively (chapter 15).
The recovery archive (items deleted during the life of the account)	30 days from deletion.	The Firm may delete permanently earlier (15.6).
Files uploaded for AI import	Deleted from the Platform's file storage immediately after reading.	Retention at the providers: Annex C.
E-mails at the e-mail provider	30 days from sending (Pro plan); the provider's backups, 7 days.	The closure of a Firm's account in Cateruno does not change the period (15.4).
The Platform's error reports	30 days.	Without the URL parameters; the browser only for those logged in.
Counting traces for limiting attempts (the IP address or its fingerprint)	At most one day; for the enquiry form, at most 48 hours.	Used only for security.
Technical logs of hosting and of the network	Lovable shows the server, function and database logs in windows of up to 5 days, but does not publish a maximum retention period; nor does Cloudflare, for the network logs. The logs may contain the IP address.	No invented common period; limited access.
Database backups	One copy per day; the maximum duration, in Annex B.	They leave rotation without current reuse; restoration reapplies the deletions.

Data	Period and starting point	Exceptions and application
Data after Account Closure	Export for 30 days or the applicable retrieval period under Regulation (EU) 2023/2854, then deletion (chapter 15).	Only the data required by law, strictly delimited, remains (15.4).
Data subject to a complaint, a dispute, an inspection or a restriction	Strictly necessary, reasoned retention, until the cause and the applicable obligations cease.	Re-examination at least every six months; after cessation, deletion according to the schedule. No general suspension for all clients.

E.2. Features marked “later”

Data	Period and starting point	Exceptions and application
The debt file (formal notices, interest calculation, evidence of dispatch and receipt)	Formal notices and the related evidence are kept in a debt file, for the period necessary for recovery, the defence of rights and the fulfilment of legal obligations. The period is set by reference to the due date, the extinguishment of obligations, the limitation period and ongoing proceedings. For a file extinguished without a dispute, the review for deletion takes place 3 years after full extinguishment.	On expiry, the file is deleted or effectively anonymised, except for documents subject to a separate legal retention requirement. Any extension is reasoned, limited to the necessary documents and reviewed periodically. The file has the review date, the reason and the period of the additional retention, the person responsible and the status of the dispute.
The voice assistant	Audio recording: no archiving after transcription; the text of the command: 30 days in the assistant’s history.	The retention of the provider, of the error queues, of the logs and of the copies is set separately before activation.
Timekeeping and any report on attendance	Set on activation (7.5).	For employee monitoring, Article 5 of Law no. 190/2018 applies.