Data Processing Addendum

Locobuzz Solutions Private Limited

Introduction

This addendum explains how Locobuzz handles personal data when you use our platform. We have tried to write it so that a non-lawyer can follow it. Where a law requires particular wording, we have kept it, but we explain it in plain terms around it.

In this addendum, "we", "us" and "Locobuzz" mean Locobuzz Solutions Private Limited. "You" means the customer that has signed the main agreement with us. The "Agreement" is that main agreement: the master subscription agreement, terms of service, order form or statement of work, whichever applies.

1. Scope and Application

1.1 This addendum forms part of the Agreement. It applies whenever we process personal data on your behalf while providing the Locobuzz platform and related services (the "Services").

1.2 It is written to meet the requirements of the laws that our customers most often operate under, including the EU and UK GDPR (in particular Article 28), the Swiss Federal Act on Data Protection, India's Digital Personal Data Protection Act 2023 and its Rules (the "DPDP Act"), and US state privacy laws such as the California Consumer Privacy Act. Together we call these "Data Protection Laws". Only the laws that actually apply to a given piece of processing are relevant to it.

1.3 If this addendum and the rest of the Agreement disagree on anything to do with personal data, this addendum wins. If the Standard Contractual Clauses (see section 9) apply and disagree with this addendum, the Standard Contractual Clauses win.

2. Definitions

We keep definitions to a minimum. These are the ones that matter:

- **Personal data** means any information about an identified or identifiable person. Under the DPDP Act this is called "digital personal data", and the person is called a "Data Principal".
- **Customer Personal Data** means personal data that we process on your behalf in providing the Services. It does not include data that we handle as a controller for our

own business, such as billing contacts and sales records, which our Privacy Policy covers.

- **Processing** means anything done with personal data, such as collecting, storing, analysing, sharing or deleting it.
- **Controller** is the party that decides why and how personal data is processed. Under the DPDP Act this is the "Data Fiduciary".
- **Processor** is the party that processes personal data on the controller's behalf. Under the DPDP Act this is the "Data Processor". Under US state laws this is a "service provider".
- **Subprocessor** means a company we engage that processes Customer Personal Data to help us provide the Services.
- **Personal Data Breach** means a breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
- **Your Users** means the people you allow to use your Locobuzz account, such as your employees, agents and agencies.

3. Roles and Responsibilities

3.1 You are the controller and we are your processor. You decide what data goes into the platform and what it is used for. We process it to provide the Services. If you are yourself acting as a processor for someone else (for example, you are an agency serving a brand), then we are your subprocessor, and you confirm that your own client has authorised you to use us.

3.2 Social networks and other platforms are not our subprocessors. Much of the data in Locobuzz comes from social networks, review sites, messaging channels and other third-party platforms that you connect to your account. Those platforms are independent controllers of the data they hold. They make it available under their own terms, and we access it through their APIs because you asked us to. The same goes for any third-party tool or channel provider that you choose to connect yourself, such as a WhatsApp business solution provider, a CRM or a helpdesk. Those providers work for you, under your own contract with them.

3.3 Your responsibilities. Because you are the controller, you are responsible for:

- having a lawful basis (or, under the DPDP Act, valid consent or a legitimate use) for the personal data you bring into the platform and for the way you use it;
- giving people any notices the law requires, including notices about your use of Locobuzz;
- following the terms of the social networks and other platforms you connect; and
- making sure your instructions to us are lawful.

4. Processing Instructions

4.1 We only process Customer Personal Data on your documented instructions. Your instructions are the Agreement, this addendum, and the way you set up and use the Services (for example, the keywords you track, the channels you connect and the reports you schedule). Any additional instruction must be agreed in writing.

4.2 If we think an instruction breaks Data Protection Laws, we will tell you. We do not have to follow that instruction until it is resolved.

4.3 If a law requires us to process Customer Personal Data in a way you have not instructed, we will tell you before we do it, unless that law forbids us from telling you.

5. Permitted Processing and Restrictions

5.1 We use Customer Personal Data only to provide, maintain, support and secure the Services for you, and to meet our legal obligations.

5.2 We do not sell Customer Personal Data. We do not share it for cross-context behavioural advertising. We do not combine it with personal data we receive from other customers or sources, except where that is needed to provide the Services you asked for.

5.3 We may create aggregated or de-identified statistics about how the platform is used (for example, system load or feature usage), so long as nobody, including you, can be identified from them. We use these to run and improve the platform.

5.4 AI features. Some features use artificial intelligence, for example to detect sentiment, classify mentions or draft replies. These run through the subprocessors listed in Annex 3 for that purpose (currently Amazon Bedrock on AWS). We do not use Customer Personal Data to train AI models that are shared with other customers, and our contracts with these subprocessors do not let them use it to train their own models.

6. Personnel and Confidentiality

6.1 Only staff who need access to do their jobs can access Customer Personal Data. Everyone with access is bound by a confidentiality obligation, and receives security and data protection training when they join and at least once a year after that.

7. Data Security

7.1 We protect Customer Personal Data with the technical and organisational measures described in Annex 2. These are designed to keep data confidential, accurate and available, and to suit the risks involved in processing it, as Article 32 of the GDPR and Rule 6 of the DPDP Rules require.

7.2 Security changes over time, so we may update these measures. We will not make a change that lowers the overall level of protection.

7.3 We hold an ISO/IEC 27001 certification and have a SOC 2 Type 2 report, each renewed through independent audit. Section 12 explains how you can see them.

8. Engagement of Subprocessors

8.1 Our current list. You give us general permission to use subprocessors. Our current subprocessors are listed in Annex 3 and on our public subprocessor page at [locobuzz.com/subprocessors]. The page shows what each subprocessor does, what data it handles and where it processes it.

8.2 How we choose and manage them. Before we use a subprocessor, we check its security and privacy practices. We sign a written contract with it that protects Customer Personal Data at least as well as this addendum does. We review our subprocessors at least once a year. We remain responsible to you for anything our subprocessors do with Customer Personal Data.

8.3 Telling you about changes. When we plan to add or replace a subprocessor, we will update the subprocessor page at least 30 days before the new subprocessor starts processing Customer Personal Data. If you subscribe to updates on that page, we will also email you. Updating the page counts as notice to you. Please subscribe, because we cannot email you otherwise.

8.4 Emergencies. If we have to replace a subprocessor urgently, for example because it has had a security incident or stopped trading, we may do so straight away. We will then update the page and tell subscribers as soon as we can.

8.5 Objecting. If you have a reasonable data protection reason to object to a new subprocessor, email privacy@locobuzz.com within 15 days of the notice. We will discuss it with you in good faith and try to find a solution, such as a different configuration or not using that subprocessor for your data. If we cannot agree a solution within 30 days, you may end the part of the Services affected by the change, and we will refund any fees you have prepaid for the remaining term of that part.

8.6 Removals. When we stop using a subprocessor, we will remove it from the page and tell subscribers. You do not need to do anything.

8.7 Customer-specific subprocessors. Some subprocessors only process data for customers who use a particular feature, such as a single sign-on connection. Annex 3 says when that is the case. A customer-specific subprocessor never sees data from customers who do not use that feature.

9. Data Location and International Transfers

9.1 Primary hosting. We host the platform and store Customer Personal Data in India, in the Amazon Web Services Mumbai region. Our production database (SingleStore Helios) also runs in Mumbai.

9.2 Other locations. A few subprocessors process limited data outside India, mostly in the United States. Annex 3 shows each one's location. We have contracts in place with each of them that include the safeguards described below.

9.3 Transfers out of the EU, UK and Switzerland. India does not yet have an EU adequacy decision. So when you send personal data from the European Economic Area to us, the EU Standard Contractual Clauses (Commission Decision 2021/914) apply, and are included in this addendum by reference. The details of which options apply are in Annex 4. In short:

- Module 2 (controller to processor) applies when you are a controller, and Module 3 (processor to processor) applies when you are a processor.
- For data from the UK, the UK International Data Transfer Addendum applies alongside the Clauses.
- For data from Switzerland, the Clauses apply with the changes Swiss law requires.

9.4 Onward transfers. When one of our subprocessors processes data in another country, we make sure the transfer is covered by a valid mechanism, such as the Standard Contractual Clauses, the EU-US Data Privacy Framework (where the subprocessor is certified), or an adequacy decision.

9.5 Transfers out of India. Under the DPDP Act, personal data can be transferred out of India unless the Government of India restricts transfers to a particular country. We will follow any such restriction, and any further conditions the Government sets for transfers.

9.6 Requests from governments. If a public authority asks us for Customer Personal Data, we will tell you before we hand anything over, unless the law forbids us from telling you. We will check that the request is lawful, push back on requests that are not, and give out only the minimum the law requires.

10. Assistance with Compliance Obligations

10.1 Requests from individuals. People have rights over their personal data, such as access, correction, erasure and, under the DPDP Act, grievance redressal and nomination. The platform includes tools that let you find, export, correct and delete data. Where those tools are not enough, we will help you respond. If someone contacts us directly about data we process for you, we will pass the request to you within five business days and will not respond to it ourselves unless you ask us to.

10.2 Impact assessments. If you need to carry out a data protection impact assessment, a DPDP data protection impact assessment, or consult a regulator, we will give you the information about the Services you reasonably need.

10.3 Records. We keep a record of the processing we carry out on your behalf, as Article 30(2) of the GDPR requires.

11. Personal Data Breach Notification

11.1 We will tell you quickly. If we become aware of a Personal Data Breach affecting Customer Personal Data, we will notify you without undue delay, and in any case within 24 hours of becoming aware of it.

11.2 What we will tell you. Our notice will explain, as far as we know at the time: what happened, what kinds of data and roughly how many people are affected, the likely consequences, what we have done and are doing about it, and who you can contact. If we do not have all the facts yet, we will send what we have and follow up as we learn more.

11.3 We will work with you. We will help you investigate, contain the breach, and meet your own duties to tell regulators and the people affected. We will not contact the regulators or the people affected about a breach of your data without talking to you first, unless the law requires us to.

11.4 What does not count. Unsuccessful attempts that do not compromise data, such as blocked login attempts, pings or port scans, are not Personal Data Breaches.

11.5 Telling you about a breach is not an admission that we were at fault.

12. Compliance Verification and Audit

12.1 Reports. Once a year, or when a regulator requires it, you can ask us for our current ISO/IEC 27001 certificate, our latest SOC 2 Type 2 report (or a bridge letter covering any gap), and a summary of our latest independent penetration test. These are confidential and are shared under the confidentiality terms of the Agreement or a non-disclosure agreement.

12.2 Questions. Once a year, we will answer a reasonable written security questionnaire from you.

12.3 Audits. If the reports and answers are not enough to show that we are complying with this addendum, or a regulator requires it, or after a Personal Data Breach affecting your data, you (or an independent auditor you appoint who is bound by confidentiality and is not our competitor) may audit us. You need to give us at least 30 days' notice and agree the scope with us in advance. Audits happen during business hours, no more than once a year (except after a breach or at a regulator's request), and without disrupting our operations or exposing other customers' data. You pay your own costs. Our infrastructure is hosted by AWS and other subprocessors, so for those parts we will rely on their independent audit reports rather than allowing on-site visits.

13. Data Return and Deletion

13.1 You can export your data. While the Agreement is in force, you can export Customer Personal Data using the platform's export tools or by asking us. Please export anything you need before the Agreement ends, because we delete Customer Personal Data soon after it ends (see section 13.2).

13.2 Then we delete it. We delete Customer Personal Data from our live systems within 7 days of the end of the Agreement. Copies in backups are deleted within 30 days of the end of the Agreement. When we finish, we confirm the deletion to you in writing.

13.3 Exceptions. We may keep data for longer only where the law requires it. Under the DPDP Rules, for example, certain logs must be kept for at least one year. Anything we keep stays protected by this addendum, and we use it only for the purpose the law requires.

13.4 Trials. If you use a free trial and do not become a paying customer, we delete trial data within 30 days of the trial ending.

14. United States State Privacy Laws

14.1 Where US state privacy laws apply, we act as your "service provider" or "processor". We will not sell or share Customer Personal Data, keep or use it for any purpose other than providing the Services, or use it outside our direct business relationship with you. We will tell you if we can no longer meet our obligations under those laws. We understand these restrictions and will comply with them.

15. Limitation of Liability

15.1 Each party's liability under this addendum is subject to the limits and exclusions of liability in the Agreement. Those limits apply to this addendum and the Agreement together, not separately. Nothing in this addendum limits either party's liability to individuals under the Standard Contractual Clauses, or any liability that cannot be limited by law.

16. General Provisions

16.1 How long this lasts. This addendum lasts as long as we process Customer Personal Data for you, even if that continues after the Agreement ends.

16.2 Changes. We may update this addendum when the law changes or to reflect changes to the Services. We will not reduce the protection it gives to Customer Personal Data during your current subscription term without your agreement. We will tell you about material changes in advance.

16.3 Governing law. This addendum is governed by the same law, and disputes go to the same courts, as the Agreement. If the Agreement does not say, the laws of India apply and the courts of Mumbai have jurisdiction. The Standard Contractual Clauses are governed by the law named in Annex 4.

16.4 Contact. For anything about this addendum or privacy, contact our Chief Data Officer, Vidyasagar Parivelli, at privacy@locobuzz.com.

Execution

By signing below, or by accepting the Agreement that refers to this addendum, the parties agree to it.

	Customer	Locobuzz Solutions Private Limited
Signature		
Name		
Title		
Date		

Annex 1: Description of Processing

This annex describes the processing, as Article 28(3) of the GDPR and Annex I of the Standard Contractual Clauses require.

Topic	Details
Parties	Data exporter (controller): the Customer named in the Agreement. Data importer (processor): Locobuzz Solutions Private Limited, Mumbai, India. Contact: privacy@locobuzz.com.
Subject matter	Providing the Locobuzz platform for social listening, customer experience and engagement, and analytics.
Duration	The term of the Agreement, plus the deletion periods in section 13.
Nature and purpose	Collecting public and owned-channel content from the sources you connect; storing it; analysing it (including sentiment, topic and

Topic	Details
	intent detection, which may use AI); routing conversations and tickets to Your Users; producing dashboards, alerts and reports; and supporting and securing the Services.
People whose data is processed	Your Users: your staff, agents and agencies who use the platform. Members of the public who post about, mention, or interact with your brands, pages or handles on social networks, review sites and other connected sources. Your customers and contacts who reach you through channels you connect, such as social messages, email, chat or messaging apps.
Types of personal data	User account data: name, work email, role, team, login and activity logs, IP address, device and browser details. Social and channel data: handles, display names, public profile details, posts, comments, replies, direct messages, images and other media, timestamps, follower counts and location where the person shared it. Case and ticket data: conversation history, notes, tags and case details. Contact data you add: names, emails and phone numbers that you upload or sync from your CRM. Derived data: sentiment, topics, intent and other labels the platform generates.
Sensitive data	We do not ask for sensitive data (such as health, religion, political opinions or sexual orientation). But people sometimes reveal it in public posts or messages, so it may end up in the platform. You should not set up the platform to target sensitive data, and should tell us if you plan to process it in a way that needs extra safeguards.

Topic	Details
Children's data	The Services are not designed for processing children's data. Some public posts may come from children. If you plan to process children's data deliberately, you must get any consent the law requires, including verifiable parental consent under the DPDP Act.
How often	Continuously, for as long as you use the Services.
How long we keep it	For the term of the Agreement, unless you delete it sooner or set a shorter retention period. After the Agreement ends, see section 13. Security and audit logs are kept for 12 months.
Subprocessors	See Annex 3.

We update this description when the platform changes in a way that affects it.

Annex 2: Technical and Organisational Security Measures

These are the main technical and organisational measures we use to protect Customer Personal Data. They are based on our ISO/IEC 27001 information security management system and are tested in our SOC 2 Type 2 audit.

Governance

- A documented information security management system, certified to ISO/IEC 27001, with policies approved by management and reviewed at least once a year.
- Named owners for information security and data protection, and regular management reviews.
- A risk assessment at least once a year, and whenever we make a significant change.

People

- Confidentiality agreements for all staff and contractors.
- Background checks before hiring, where local law allows.
- Security and data protection training when people join and at least once a year after that, including secure coding training for engineers.
- Access removed promptly when someone leaves or changes role.

Access control

- Access based on role and the principle of least privilege.
- Single sign-on for internal systems and cloud consoles through a central identity provider, with multi-factor authentication required.
- A separate, tightly controlled process for privileged access, with approval and logging.
- Access to production networks through a VPN.
- A strong password policy, account lockout and session timeouts.
- User access reviews at least every quarter.

Encryption

- Data encrypted in transit using TLS 1.2 or higher.
- Data encrypted at rest using AES-256, including databases, file storage and backups.
- Encryption keys managed in AWS Key Management Service, with access restricted and rotation in place.
- Full-disk encryption on staff laptops.

Application security

- A secure development process: peer review of every code change, approval before deployment, and automated build and deployment pipelines.
- Separate development, testing and production environments. Personal data is masked or not used in non-production environments.
- Independent penetration testing of the platform at least once a year, with findings fixed according to their severity.

Infrastructure and operations

- Systems hardened in line with CIS benchmarks.
- Regular vulnerability scanning and patching, with critical issues fixed as a priority.
- Firewalls and security groups, with firewall rules reviewed regularly.
- Logging and monitoring of systems for unusual activity. Security logs kept for 12 months.

Availability and recovery

- Hosting across multiple AWS availability zones in the Mumbai region.
- Regular automated backups, encrypted and tested at least every quarter.
- A business continuity and disaster recovery plan, aiming to restore service within 24 hours of a major failure, tested at least once a year.

Incident response

- A documented incident response process with a trained response team.
- Customer notification as set out in section 11.
- A review after every significant incident to find the root cause and stop it happening again.

Subprocessors

- Security and privacy review before we engage a subprocessor.
- Written contracts with data protection terms at least as protective as this addendum.
- A review of each subprocessor at least once a year, including its certifications or audit reports.

Physical security

- Production systems are hosted in AWS data centres, which have strong physical controls that are independently audited (AWS ISO 27001 and SOC 2).
- Our offices have controlled entry and CCTV. No customer data is stored on office servers.

Data minimisation and deletion

- Retention periods for each type of data, and secure deletion at the end of them, as described in section 13.
- Tools that let customers delete data and handle individuals' requests.

Annex 3: Authorised Subprocessors

These are the subprocessors we use as of the date of this addendum. The latest list is always on our subprocessor page at [locobuzz.com/subprocessors]. See section 8 for how we tell you about changes.

Subprocessor	What they do for us	Personal data they handle	Where	Notes
Amazon Web Services, Inc. (including Amazon Bedrock)	Cloud hosting, storage and AI model inference for platform features	All Customer Personal Data	Mumbai, India	Our core infrastructure. Amazon Bedrock runs the AI features in the platform. We buy AWS through a reseller (Minfy), which has no access to customer data.

Subprocessor	What they do for us	Personal data they handle	Where	Notes
SingleStore, Inc. (SingleStore Helios)	Managed production database	Customer data, including mentions and tickets	Mumbai, India	Runs on AWS in the Mumbai region.
Mailgun Technologies, Inc.	Sending emails from the platform	Recipient email addresses and email content	United States	Used for alerts, scheduled reports and notifications.
PDFmyURL (billed through FastSpring B.V.)	Turning dashboard reports into PDFs	Content of the reports being converted	United States, European Union, Singapore	We are replacing this with an in-house service. We will remove it from this list and tell subscribers when that happens.
WorkOS, Inc.	Single sign-on (SSO) connection	Your Users' names, email addresses and login data	United States	Customer-specific: only processes data for customers who sign in through a WorkOS SSO connection. We are replacing this with an in-house service.

FastSpring B.V. only handles billing between Locobuzz and PDFmyURL and does not receive Customer Personal Data.

Annex 4: International Data Transfer Provisions

This annex sets out the options chosen in the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), the UK Addendum and the Swiss modifications, where section 9.3 applies.

EU Standard Contractual Clauses

Clause	What applies
Module	Module 2 (controller to processor) where you are a controller. Module 3 (processor to processor) where you are a processor.
Clause 7 (docking clause)	Included.
Clause 9 (subprocessors)	Option 2, general written authorisation. We will give at least 30 days' notice of changes, as section 8 describes.
Clause 11 (redress)	The optional wording on independent dispute resolution does not apply.
Clause 13 (supervision)	The supervisory authority of the EU member state where you are established. If you are not established in the EU, the authority of the member state where your EU representative is located, or otherwise the Irish Data Protection Commission.
Clause 17 (governing law)	The law of Ireland.
Clause 18 (courts)	The courts of Ireland.
Annex I (parties and processing)	As set out in Annex 1 of this addendum.
Annex II (security)	As set out in Annex 2 of this addendum.
Annex III (subprocessors)	As set out in Annex 3 of this addendum and on our subprocessor page.

UK transfers

For personal data from the United Kingdom, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, issued by the UK Information Commissioner) applies. Table 1 is completed with the parties' details in Annex

1. Tables 2 and 3 are completed with the information in this annex and Annexes 1 to 3. For Table 4, neither party may end the UK Addendum when it changes.

Swiss transfers

For personal data from Switzerland, the EU Standard Contractual Clauses apply with these changes: references to the GDPR mean the Swiss Federal Act on Data Protection; the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and the term “member state” includes Switzerland, so that people in Switzerland can bring claims there.