Locobuzz Privacy Policy

Locobuzz Solutions Private Limited and its affiliated entities ("**Locobuzz**" or "**We**" or "**Our**" or "**Us**") are committed to ethical conduct, prioritizing the protection of Your Personal Information. Guided by principles of integrity, client focus and care, Our approach to data privacy is integral to Our business operations, influencing Our decision-making processes, products, and innovation, with a staunch emphasis on privacy and respect.

This Policy is meticulously crafted to articulate the types of Personal Information we handle, the ways in which we collect it, and the purposes behind our processing and utilization of this information, particularly in our role as a service provider. It's important to note that Our Services are specifically designed for use by corporate entities rather than for personal, family, or household purposes. As such, we consider any Personal Information provided to us as being related to individuals in their professional capacity, representing their respective businesses.

1. **Definitions**
   For the purpose of this Policy:

a. "**Customer"** shall mean any organization or business that is a client of Locobuzz, has purchased Locobuzz's Products and/or Services, and has authrized its users to engage on the Locobuzz Platform.
b. "**Personal Information**" shall mean information that relates to an identified or identifiable individual.
c. "**Our Products**" or "**Our Services**" or "**Our Platform**" shall mean Locobuzz's comprehensive suite of Customer experience management solutions, including products, modules, platform, services, as well as demos and trials, designed for social engagement. These offerings enable customers to connect with, engage, and service their clientele using publicly available online data. We also provide support services like enablement, success management, transformation, analytics, and moderation to meet Ourcustomers' diverse needs. The term "**Products**", "**Platform**" and/or "**Services**" within this Policy shall mean all elements of Locobuzz's offerings and any future versions or updates.
d. "**We**" "**Us**" "**Our**" or "**Locobuzz**" means Locobuzz Solutions Private Limited, Business Square, C 301, Chakala, Andheri East, Mumbai, Maharashtra 400093 and Our affiliated or group companies.
e. "**You**" or "**Your**" shall mean the individual reading this, their organization, or the individual whose Personal Information is being processed, as well as the user engaging with or employing the Platform, or the organization, or other legal entity on behalf of which such user is utilizing the Platform, as applicable.

2. **Scope of this Policy and Locobuzz's Role**

a. As a service provider and processor, Locobuzz functions as an advanced customer user experience tool for businesses, facilitating efficient oversight and evaluation of social media content. The Platform offers a comprehensive monitoring dashboard for tracking keywords, influencers, and competitors, enhancing operational efficiency through organizational dashboard sharing. Focused on indexing publicly available information, We aggregate content from a variety of sources, including major social media platforms and digital channels, while respecting user privacy settings on these platforms. Security measures are in place to safeguard the Platform's use, though responsibility for the application of its Services rests with Our Customers.

b. Locobuzz provides six essential features for comprehensive customer user experience: Analytics, Audience, Engagement, Listening, Governance, and Integration. These features enable customers to analyze brand performance, streamline engagement, manage multilingual conversations, monitor trends, and integrate with other systems for a cohesive marketing strategy.

c. As a processor, We support customers in managing digital customer experiences and marketing strategies, ensuring compliance with data processing laws. When acting as a processor, We adhere to contractual obligations, ensuring data security and processing limits as agreed with Our customers. Customers maintain control over the personal data processed on Our Platform, with Locobuzz adhering to agreed security and processing standards. For concerns regarding data managed by Our Platform, inquiries should be directed to the respective customer, in line with their privacy policy.

For information on data handling by entities You engage with, consult their direct communications or review their privacy policies.

3. **Data Processing Activities and Legal Basis**

While rendering Our Services, we operate strictly as a Data Processor across all jurisdictions, conducting operations like social listening, analytics, and AI engagement on behalf of Data Controllers. Our compliance with global laws is underpinned by contractual agreements that specify processing details and security obligations. These agreements align with the legal bases established by Data Controllers, encompassing consent, withdrawal rights, and contractual necessity. Our approach ensures compliance through rigorous protocols, meticulous record-keeping, and advanced security measures, supporting Data Controllers in upholding data subjects' and consumers' rights while maintaining data integrity and confidentiality.

The Locobuzz Mobile App, available on the Google Play Store, is designed exclusively for Our customers. Non-customers are advised to uninstall the app.

4. **Collection and usage of Personal Information by Locobuzz**

At Locobuzz, we gather and utilize various categories of personal information to enhance user experiences and provide valuable insights to our clients. We source information from social media content, public engagement metrics, and client websites/apps. Our priority is to responsibly utilize this data to deliver personalized experiences while ensuring user privacy and security.

a. **What data do we process?**

i. **Specific Categories of Personal Informations:**
   1. Identifiers (name, IP address, online identifiers)
   2. Internet or network activity information (browsing history)
   3. Geolocation data
   4. Inferences drawn from collected data (interests, preferences)

ii. **From Social Media Content**
   1. Public profile information (name, profile picture, bio)
   2. Public user-generated content (posts, tweets, comments, etc.)
   3. Publicly shared location data (if enabled)
   4. Public engagement metrics (likes, shares, comments)

iii. **From Client websites/Apps:**
   1. Usage data (pages visited, time on page)
   2. Device information (IP address, browser type)

b. **Why We Process Your Data**

Locobuzz engages in the processing of your data with a multifaceted approach aimed at enhancing the efficacy and personalization of Our Services. Our primary objectives include:

i. **Social Media Analytics**: We delve into the vast landscape of social conversations to extract meaningful insights about brand sentiment, gauge competitor trends, and understand the public perception surrounding your brand. This involves a meticulous analysis aimed at distilling valuable information from social media chatter to inform strategic decisions.

ii. **Customer Engagement:** By analyzing customer interactions and feedback, we identify pivotal issues and opportunities that enable us to tailor communication strategies effectively. This process is crucial for fostering improved engagement by addressing customer needs directly and personalizing the user experience.

iii. **Platform Improvement:** Understanding user behavior is key to optimizing the design and functionality of our Platform. By processing data related to how users interact with our platform, we can make informed adjustments that enhance the overall user experience, ensuring it is intuitive, engaging, and aligned with user expectations.

iv. **Marketing Insights:** We provide data-driven insights to help businesses refine their marketing strategies and campaigns. By analyzing customer demographics, engagement metrics, and campaign effectiveness, We enable targeted marketing efforts that resonate with the audience and drive conversions.
v. **AI and Automation**: We utilize AI and automation technologies to process and analyze large volumes of data efficiently. This includes natural language processing (NLP), sentiment analysis, predictive analytics, and machine learning algorithms to automate tasks, extract insights, and optimize workflows.
vi. **Data-driven Decision Making**: We empower businesses to make informed decisions based on data-driven insights. By aggregating and analyzing data from various sources, We provide actionable intelligence that helps businesses identify opportunities, mitigate risks, and stay ahead of the competition.

c. **With whom we share**

At Locobuzz, we value the trust you place in us to handle your data responsibly. Our data sharing practices are designed with the utmost consideration for privacy and legal compliance.

i. **With Clients**: We share processed data, including insights and analytics, exclusively with our clients. This sharing is integral to the services we provide and is conducted within the strict boundaries of our contractual agreements. Every effort is made to ensure that data is shared in a manner that respects the privacy of the individuals it pertains to and adheres to our mutual confidentiality obligations.
ii. **Subprocessors**: To extend the functionalities of Our Services, we engage with subprocessors. These entities are carefully vetted to confirm their adherence to data protection standards that match or exceed our own. Data shared with sub processors is limited to what is essential for the provision of Our Services, and is governed by contractual measures that enforce our privacy and security standards. For more information, check clause 9 of this Policy.

d. **How We Protect Your Data**

We employs a multifaceted approach to safeguard your personal data against unauthorized access, loss, or misuse. Our commitment is rooted in the principles of transparency, accuracy, relevance, and controlled sharing. Below, we detail our comprehensive measures:

i. **Encryption**: We ensure the security of your data both in transit and at rest, utilizing TLS for data in transit and AES-256 encryption for data at rest.
ii. **Access Controls**: Access to sensitive data is regulated through role-based access controls, reinforced by mandatory multi-factor authentication to prevent unauthorized access.
iii. **Activity Logging**: For auditing and monitoring purposes, access to sensitive data is meticulously logged.

iv. **Vulnerability Management**: We conduct regular vulnerability scans and penetration testing to identify and remediate potential security vulnerabilities.
v. **Employee Training**: Our employees undergo rigorous security awareness training to foster a culture of data protection and understand best practices in data security.
vi. **Data Integrity**: We process your information strictly for its intended purposes, ensuring the data remains accurate, up-to-date, and is only shared with your consent or under specific agreements that safeguard international data transfers.
vii. **Internal Audits:** Conduct periodic internal audits to assess compliance with this policy and identify any security risks.

5. **Transferring Personal Data Across Borders**

In our pursuit of a seamless digital experience, we understand the importance of transferring personal data across borders, encompassing regions such as India, the United States, the European Union, and beyond, to continually improve and enhance Our Services. Recognizing the diversity of privacy regulations globally, we adhere to strict protocols to ensure compliance and protection for your data during international transfers, transferring data only in accordance with contractual obligations. We transparently share information about third-party involvement and commit to implementing necessary measures, including standard contractual clauses, to maintain data security and privacy across jurisdictions. Additionally, we ensure that our partners uphold similar standards to safeguard your personal information effectively.

6. **Data Privacy for Minors**

Our operations do not target minors. We are committed to upholding minors' privacy online, adhering to relevant legislation. Should We inadvertently collect data from individuals under 18, We will either delete this information promptly or inform the customer involved.

7. **Security Measures and Data Breach Notification**

We maintain stringent security protocols across all jurisdictions to safeguard personal data from unauthorized access, loss, or damage, employing comprehensive technical and organizational strategies. In the event of a data breach, we are committed to promptly notifying relevant customers within the specified timeframe or, if feasible, within 72 hours of discovery. Furthermore, we endeavor to directly inform affected individuals without delay if their rights and freedoms are significantly at risk, providing detailed information about the breach and recommended measures to mitigate potential adverse effects, in compliance with global requirements.

8. **Data Purge Policy**

In adherence to our commitment to data privacy and protection, we implement a strict data retention policy. All personal data held in our records and systems will be deleted within 1 (one)

month after the cessation of the customer relationship or termination of agreement with Locobuzz, in line with data minimisation and retention principles. This approach ensures that we adhere to data protection standards, respecting the privacy rights of our clients by eliminating unnecessary data retention. Our process for data deletion is designed to permanently remove your data, preventing any future access or use.

9. **Sub-processor Engagement**

We ensure diligent engagement with sub-processors across all jurisdictions, requiring them to adhere to the same data protection standards and obligations as Us. This engagement is governed by contractual terms, with sub-processors only engaged with prior written consent from Data Controllers. A maintained list of sub-processors is available upon request, ensuring transparency and accountability in the processing chain and upholding the integrity and security of personal data.We use the following subprocessors:

a. **Cloud Infrastructure Partners:**

i. **Amazon Web Services (AWS):** Provides core infrastructure services including computing, storage, databases, and networking. AWS ensures the scalability, reliability, and security of Our Platform.

ii. **Microsoft Azure**: Offers core infrastructure services such as computing, storage, databases, and networking. Azure contributes to the robustness and resilience of Locobuzz's platform.

b. **Analytics and Monitoring Tools:**

i. **Google Analytics:** Offers web analytics services for tracking website/app usage patterns and user behavior. Google Analytics provides insights to optimize user experience and engagement on Our Platform.

ii. **Datadog:** Provides log management, infrastructure monitoring, and application performance monitoring to ensure service reliability and identify potential issues. Datadog Analytics aids in maintaining the performance and stability of Locobuzz's platform.

c. **Integration Tools:**

i. **Quickwork:** Assists in creating automated workflows between different apps and services, streamlining business processes. Quickwork facilitates seamless integration and data flow within Locobuzz's platform, enhancing operational efficiency and productivity.

10. **Data Sharing and Usage Disclaimer**

In delivering Our Services, we may share certain information with clients to fulfill our contractual obligations. This information sharing is central to the provision of Locobuzz services and may include, but is not limited to, social media content, demographic information, and other insights. It's important to note that demographic information is only collected and shared with explicit

consent from the individuals involved. This disclaimer serves to transparently communicate the nature of data sharing involved in Our Services, ensuring that users are informed about how their data might be utilized.

11. **Amendments to this Privacy Policy**

    Our Privacy Policy, and any Supplementary Policies undergo regular reviews and updates to reflect changes in legal requirements, technological advancements, or operational procedures. It's designed to complement Locobuzz's primary Privacy Policy, ensuring a comprehensive understanding and compliance with our data processing practices. This integrated approach ensures our policy remains current and fully aligned with global data protection standards.

12. **Consent**

    By providing personal data to us across all jurisdictions, you consent to the processing and use of personal data as outlined in our Privacy Policy. Your consent is recognized as freely given, specific, informed, and unambiguous. We commit to retaining evidence of such consents, ensuring compliance with applicable laws highlighting our dedication to lawful and transparent data processing practices globally.

    For personal data access, individuals can contact Locobuzz Privacy Compliance with their request details via email at privacy@locobuzz.com or by mailing to Locobuzz Private Ltd, C- 301, Chakala, Business Square, Andheri East, Mumbai, Maharashtra 400093.

    For detailed information regarding your rights and our obligations, tailored to the country of your residence, please refer to the supplementary policies attached corresponding to your jurisdiction.

EU/EEA Notice

Our European Union (EU) / European Economic Area (EEA) / United Kingdom (UK) Privacy Supplementary Notice (**EU/EEA Notice**) in alignment with the General Data Protection Regulation 2018 (**GDPR**). It details our protocols for managing Personal Information and the rights of individuals under GDPR. Additionally, as a Data Processor under GDPR, we outline our commitments and practices for processing personal data of EU citizens in compliance with GDPR requirements.

Definitions:

- "**Data Subjects**" refers to any individual who is the subject of Personal Data.
- **"Personal Data**" refers to any information relating to a person that can be used to directly or indirectly identify them. This includes, but is not limited to, information such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- "**Data Controllers**" shall mean Locobuzz's paid customers;
- "**Data Processors**" or "**We**" shall mean Locobuzz Solutions Private Limited

Data Subject Rights

Data subjects have the right to access, correct, restrict processing of, and erase their personal data. They also have the right to data portability, to object to processing, and to withdraw consent at any time. We support our Data Controllers in facilitating these rights, ensuring data subjects can easily exercise them.

- **Access**: Data subjects can request a copy of their personal data, learning about its use and who it's shared with, sometimes subject to a fee for multiple requests.
- **Correction**: Inaccurate or incomplete data can be corrected upon the data subject's request.
- **Restriction**: Processing can be limited under certain conditions, offering data subjects control over their data.
- **Portability**: Data subjects can receive their data in a structured format and transfer it to another entity.
- **Objection**: The right to object allows data subjects to refuse certain types of processing.
- **Withdrawal of Consent**: Data subjects can retract their consent, impacting the legality of processing activities based on that consent.
- **Erasure**: Known as the right to be forgotten, this allows data subjects to have their data deleted under certain circumstances.

Data Controller Obligations

Data Controllers are responsible for ensuring lawful and transparent data processing, obtaining consent where necessary, protecting data via security measures, and adhering to data subjects' rights. They

must also conduct data protection impact assessments (DPIAs) for high-risk processing, report data breaches promptly.

Data Processor Obligations

As a Data Processor, We adhere to documented instructions from our Data Controllers, implementing appropriate technical and organizational measures to secure personal data, and engaging sub-processors only with prior authorization. We collect and retain personal data in accordance with GDPR requirements, ensuring relevance to the specified purpose and adherence to specific retention periods based on data nature, operational needs, and legal and contractual obligations, preventing indefinite retention without justification.

Cross-border Data Transfer

For any transfer of personal data outside the EU, We employ appropriate safeguards such as standard contractual clauses and adherence to corporate binding rules, ensuring the protection of personal data in line with GDPR requirements.

Children's Data

We provide special protection for children's data, requiring parental consent for processing activities involving individuals under the age of 16, in accordance with member state laws.

India Supplementary Privacy Notice under the DPDP Act

Our Indian Privacy Supplementary Notice (**India Notice**) in alignment with the Digital Personal Data Protection Act, 2023 (**DPDP Act**). It details our protocols for managing Personal Information and the rights of individuals under the DPDP **Act**. Additionally, as a Data Processor under the **DPDP Act**, Locobuzz Solutions outlines its commitments and practices for processing personal data of Indian citizens in compliance with **DPDP Act** requirements.

Definitions

- **"Data Principals"**: refers to any individual whose Personal Data we process.
- **"Personal Data"** refers to any information relating to a person that can be used to directly or indirectly identify them. This includes, but is not limited to, information such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- **"Data Fiduciaries"**: shall mean Locobuzz's paid customers
- "**Data Processors**" or "**We**" shall mean Locobuzz Solutions Private Limited

Rights of Data Principals

The DPDP Act empowers Data Principals with several rights, including but not limited to:

- **Right to Access**: Data Principals can request access to their Personal Data to understand how and why it is processed.
- **Rights to Correction and Erasure**: Data Principals have the right to request corrections to inaccurate or incomplete Personal Data, and under certain conditions, they can also request the deletion of their data, known as the 'right to be forgotten.'
- **Grievance Redressal:** Data Principals can lodge complaints regarding the processing of their Personal Data, ensuring accountability and transparency in data processing activities.

Obligations of a Data Controller

The data controller must process Personal Data in a fair and reasonable manner that respects the privacy of the Data Principal. This includes providing notice to Data Principals before or at the time of data collection, ensuring transparency and informed consent. Additionally, the data controller is tasked with maintaining data quality by ensuring that the collected data is accurate and used for purposes relevant to the reasons it was collected. Furthermore, the data controller must adhere to data storage limitation principles, retaining data only as long as necessary for the purposes it was collected, thereby safeguarding against unnecessary data retention and ensuring compliance with relevant regulations.

Obligations of Data Processors

As a Data Processor, We adhere to stringent guidelines to protect Personal Data, working closely with Data Fiduciaries to ensure:

- **Fair and Reasonable Processing**: Personal data is processed in a manner that respects the privacy of Data Principals.
- **Data Quality and Storage Limitation:** Data collected is relevant, accurate, and retained only for the duration necessary for the purposes for which it was collected.
- **Security Safeguards:** We implement robust security measures to protect Personal Data from unauthorized access, disclosure, or destruction.

Cross-border Data Transfer

The transfer of Personal Data outside India is conducted under strict conditions, ensuring that such transfers provide a level of protection compliant with the DPDP Act. We employ mechanisms like standard contractual clauses to safeguard Personal Data during cross-border transfers.

Children's Data

We recognize the importance of protecting children's Personal Data, requiring verifiable parental consent for processing activities involving individuals under the age of 18, in strict compliance with the DPDP Act.

Supplementary Privacy Policy for California

Our California Privacy Supplementary Notice ("California Notice") serves as an additional document to our primary Notice and is exclusively tailored for individuals residing in California, in alignment with the California Consumer Privacy Act (CCPA). It provides comprehensive insights into our protocols for managing Personal Information, while also detailing the extensive rights afforded to California residents under these legislations.

Definitions

- "**Business**" specifically pertains to Locobuzz's paid Consumers, for whom data processing services are provided.
- "**Consumer"** refers to any natural person being a California resident, who is identified or identifiable through Personal Data that is processed by a Data Controller.
- **"Personal Data**" refers to any information relating to a person that can be used to directly or indirectly identify them. This includes, but is not limited to, information such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- "**Service Provider**" or "**We**" shall mean Locobuzz Solutions Private Limited.

Consumer Rights

Consumers in the California enjoy comprehensive rights under the Personal Data Protection Law, including:

- **Transparency in Personal Information Handling:** Consumers can request disclosure of the specific pieces of personal information collected about them and the purposes for which their information is used and shared.
- **Restriction and Deletion:** Consumers have the right to request the deletion of their personal information, with certain exceptions as mandated by law.
- **Opt out of the sale:** Consumers can opt-out of the sale of their personal information, although, We do not sell personal information as part of its service offerings.
- **Non-Discrimination:** Consumers have the right to non-discrimination for exercising their CCPA rights.

Business Obligations

In the capacity of Business as defined herein, our clients bear the responsibility of ensuring compliance with California's data protection laws, which entails implementing sufficient security measures to safeguard Personal Data from unauthorized access, alteration, disclosure, or destruction. They are obligated to issue notices to consumers either at the time of or prior to the collection of personal

information, establish protocols to address consumer requests for exercising their rights under the CCPA, and retain records of such requests and the business's responses for a minimum of 24 months.

Data Processor Obligations

As a Data Processor, We adhere to using personal information solely for the contracted services' specified purposes. We refrain from retaining, using, or disclosing data beyond the contract's scope. Our operations prioritize security measures to prevent unauthorized processing or loss of Personal Data. Engagement with sub-processors entails their compliance with equivalent data protection standards to maintain data integrity and confidentiality.

Cross-border Data Transfer

Transfers of Personal Data outside California will only occur subject to contractual clauses or the Consumer's consent under conditions that ensure an adequate level of protection.

Children's Data

We are committed to protecting the privacy of children's data and will take appropriate steps to ensure compliance with California's data protection laws in this regard.

Supplementary Privacy Policy for the United Arab Emirates (UAE)

Our United Arab Emirates (**UAE**) Privacy Supplementary Notice (**UAE Notice**) in alignment with the Personal Data Protection Law, 2022 (**PDPL Act**). It details our protocols for managing Personal Information and the rights of individuals under the PDPL Act. Additionally, as a Data Processor under the PDPL Act, We outline our commitments and practices for processing personal data of UAE citizens in compliance with the PDPL Act requirements.

Definitions

- "**Data Principal" or "Data Subjects"** refers to any natural person who is identified or identifiable through Personal Data that is processed by a Data Controller.
- **"Personal Data**" refers to any information relating to a person that can be used to directly or indirectly identify them. This includes, but is not limited to, information such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- "**Data Controllers**" shall mean Locobuzz's paid customers;
- "**Data Processors**" or "**We**" shall mean Locobuzz Solutions Private Limited.

Data Principal Rights

Data Subjects in the UAE enjoy comprehensive rights under the Personal Data Protection Law, including:

- **Access:** Individuals can access their Personal Data and obtain detailed processing information.
- **Correction and Erasure:** Individuals may request correction of inaccurate or incomplete data and deletion from our records.
- **Restrict Processing:** Individuals can request a restriction on the processing of their Personal Data in specific circumstances.
- **Data Portability:** Individuals have the right to receive their Personal Data in a structured, commonly used, and machine-readable format.
- **Object:** Individuals have the right to object to the processing of their Personal Data, particularly in cases of direct marketing.

Data Controller Obligations

As the Data Controller, our clients are responsible for ensuring compliance with UAE's data protection laws, including implementing adequate security measures to protect Personal Data against unauthorized access, alteration, disclosure, or destruction. They must maintain comprehensive records of data processing activities and conduct Data Protection Impact Assessments (DPIA) for high-risk processing activities. Additionally, our clients are obligated to promptly report any data breaches to the competent authorities within the UAE.

Data Processor Obligations

As a Data Processor, We are committed to processing Personal Data strictly according to the Data Controller's instructions, ensuring adherence to specified guidelines. We prioritize the implementation of appropriate security measures to safeguard Personal Data from unauthorized or unlawful processing, as well as accidental loss, destruction, or damage. Additionally, any engagement of sub-processors will be subject to the condition that they agree to comply with equivalent data protection obligations, maintaining the integrity and confidentiality of the data entrusted to them.

Cross-border Data Transfer

Transfers of Personal Data outside the UAE will only occur subject to contractual clauses or the data subject's consent under conditions that ensure an adequate level of protection.

Children's Data

We are committed to protecting the privacy of children's data and will take appropriate steps to ensure compliance with the UAE's data protection laws in this regard.

Supplementary Privacy Policy for South East Asia (Thailand)

Our Thailand Privacy Supplementary Notice ("Thailand Notice") serves as an additional document to our primary Notice and is exclusively tailored for individuals residing in Thailand, in alignment with the Personal Data Protection Act, 2022 ("PDPA"). It provides comprehensive insights into our protocols for managing Personal Information, while also detailing the extensive rights afforded to Thailand residents under these legislations.

For the purpose of this Supplementary Notice,

- "**Data Subjects**" refers to any individual who is the subject of Personal Data.
- **"Personal Data"** refers to any information relating to a person that can be used to directly or indirectly identify them. This includes, but is not limited to, information such as name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- "**Controllers**" shall mean Locobuzz's paid customers;
- "**Processors**" or "**We**" shall mean Locobuzz Solutions Private Limited;

Data Processing Activities and Legal Basis

While rendering our Services to our Customers, We process Personal Data strictly as a Data Processor, conducting operations like social listening, analytics, and AI engagement on behalf of Data Controllers, in compliance with PDPA. Under the PDPA, our approach encompasses rigorous compliance with contractual obligations, executing tasks in the interest of the general public, and robust data protection protocols to safeguard Personal Data and support Data Controllers in upholding Data Subjects' rights. This ensures all parties uphold PDPA requirements through clearly defined roles and responsibilities. We retain data only as necessary, maintaining its integrity and confidentiality through advanced security measures, underscoring our commitment to data protection excellence and regulatory compliance.

Data Subjects Rights

Data Subjects in Thailand enjoy comprehensive rights under the Personal Data Protection Act, 2022, including:

- **Informed Consent**: Detailed information on data collection, usage, retention, and controller details.
- **Access**: The ability to access and receive a copy of your Personal Data.
- **Data Portability**: Transferring data to another entity, where applicable.
- **Objection**: The right to object to data processing in certain circumstances.
- **Erasure**: Request deletion or anonymization of your data under specific conditions.

- **Withdraw Consent**: Withdraw your consent to data processing at any time, with certain exceptions.
- **Restrict Processing**: Pause the use of your data under specific circumstances.
- **Rectification**: Correct inaccurate or incomplete data.

Data Controller's Rights

As a data controller, our clients possess various rights, including the issuance of instructions concerning the specifics of Personal Data processing, mandating security measures to safeguard Personal Data, conducting audits to ensure compliance with data protection regulations, controlling the engagement of sub-processors to manage data processing effectively, being promptly notified of any breaches involving Personal Data, and retaining the authority to terminate contracts in cases of non-compliance.

Data Processor Obligations

In our data handling, we strictly adhere to Data Controller directives and PDPA laws, ensuring lawful and purpose-specific data usage. Robust security measures like encryption and secure storage prevent unauthorized access and data loss. We promptly notify stakeholders in case of breaches, facilitate data subject rights, and obtain transparent consent for data processing. We handle international transfers carefully and cooperate with audits, ensuring data accuracy and confidentiality. Our data collection is purpose-limited, and we respect deletion requests, utilizing anonymization for privacy protection. These practices demonstrate our commitment to protecting Personal Data, ensuring compliance with PDPA and other regulatory requirements, and upholding the privacy and security of the data entrusted to us.

Cross-border Data Transfer

The transfer of Personal Data beyond the borders of Thailand is contingent upon the existence of robust measures ensuring an adequate level of protection and the implementation of appropriate safeguards.

Sub-processor Engagement

Our engagement with sub-processors is conducted with due diligence and under contractual terms that require them to adhere to the same data protection standards as Us, ensuring the integrity and security of Personal Data throughout the processing chain.

Children's Data

We are committed to protecting the privacy of children's data and will take appropriate steps to ensure compliance with Thailand's data privacy laws in this regard.