JFROG CLOUD DATA PROCESSING ADDENDUM

This **JFrog Cloud Data Processing Addendum** ("**DPA**") forms part of the **JFrog Cloud Terms and Conditions** available at https://jfrog.com/cloud-terms-and-conditions/ or entered by and between JFrog and Customer (the "**Agreement**"). Both Parties shall be referred to as "**Parties**". Any capitalized terms which are not defined herein, shall have the meaning ascribed to them in the Agreement.

To the extent JFrog ("**JFrog**", "**Processor**" or "**Service Provider**") Processes any Personal Data on behalf of the Customer ("**Customer**", "**Controller**" or "**Business**") in connection with the JFrog Platform, the provisions of this DPA shall apply.

1. DEFINITIONS

In this DPA, the following terms will have the meanings set out below:

1.1. "**Controller**", "**Member State**", "**Process/Processing**", "**Processor**", "**Special Categories of Personal Data**", "**Business**", "**Consumer**", "**Personal Information**", "**Sell**", "**Share**" and "**Service Provider**" shall have the same meaning as defined in Data Protection Laws;

1.2. "**Data Protection Laws**" means (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data ("**GDPR**"); (ii) **UK Data Protection Laws** which means the Data Protection Act 2018, and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) ("**UK GDPR**"); and (iii) **California Data Protection Laws** which means the California Consumer Privacy Act of 2018, California Civil Code § 1798.100 et seq. ("**CCPA**") including as modified by the California Privacy Rights Act of 2020 and its implementing regulations ("**CPRA**"), as amended, or superseded from time to time, and as applicable to the Processing of Personal Data under this DPA;

1.3. "**Data Subject Request**" means a request from a Data Subject to exercise applicable rights under Data Protection Laws;

1.4. "**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**") Processed by JFrog on behalf of the Controller under this DPA and the Agreement;

1.5. "**Restricted Transfer**" means a transfer of Personal Data from Controller to Processor, to a jurisdiction outside of the European Economic Area ("**EEA"**) and/or the United Kingdom of Great Britain and Northern Ireland ("**UK**"), unless such transfer is made to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant authorities of the EEA and/or the UK as relevant ("**Adequacy Decision**");

1.6. "**Security Breach**" means a breach of security leading to any unauthorized, accidental or unlawful destruction, loss, alteration, disclosure of, or access to Personal Data which has been validated by JFrog;

1.7. "**Standard Contractual Clauses**" means (i) the standard contractual clauses for the transfer of Personal Data to third countries which do not ensure an adequate level of protection as set out by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 under the GDPR as updated, amended, replaced or superseded from time to time by the European Commission ("**EU SCCs**"); and (ii) Standard Data Protection Clauses issued by the UK Information Commissioner's Office ("**ICO**") under S119A(1) of Data Protection Act 2018, to the SCCs, for parties making Restricted Transfers ("**UK Addendum**"), collectively "**SCCs**"; and

1.8. "**Supervisory Authority**" means, as applicable, an appointed government entity with the authority to enforce Data Protection Laws, including, but not limited to (i) an independent public authority which is established by a Member State pursuant to the GDPR; and (ii) the ICO in the UK.

2. DETAILS OF PROCESSING

The Parties acknowledge that the Processing of Personal Data by JFrog is for the provision of the JFrog Platform pursuant to the Agreement. The nature and purpose of the Processing, as well as the duration of the Processing, the types of Personal Data, and categories of Data Subjects whose Personal Data shall be Processed under this DPA, are detailed in **Appendix 1**. Such Personal Data is disclosed and transferred for the Permitted Purposes as set forth in this DPA.

3. DISCLOSING OF PERSONAL DATA

Controller will:

3.1. only have JFrog Process Personal Data in accordance with the requirements of the applicable Data Protection Laws;

3.2. only disclose Personal Data to the JFrog for one or more defined purposes which are consistent with the terms of the Agreement ("**Permitted Purposes**");

3.3. have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data;

3.4. where required under Data Protection Laws, ensure that a notice has been made available to the relevant Data Subjects informing them that their Personal Data will be disclosed to the JFrog or to a category of third party describing JFrog; and

3.5. not disclose any Special Categories of Personal Data to JFrog.

4. PROCESSING OF PERSONAL DATA

In its capacity as a Processor, JFrog will:

4.1. only Process Personal Data on behalf of and in accordance with Controller's reasonable instructions as detailed in this DPA;

4.2. not Process Personal Data in a way that is incompatible with, or for longer than is necessary to carry out, the Permitted Purposes (other than to comply with a requirement of applicable law to which JFrog is subject);

4.3. ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have executed written confidentiality agreements and received appropriate information security and privacy training on their responsibilities;

4.4. maintain an information security program designed to implement appropriate Technical and Organizational Measures ("**TOMs**") to protect Personal Data against a Security Breach as detailed in Section 7 below (Security Responsibilities); and

4.5. reasonably assists Controller to facilitate the fulfillment of Controller's obligation to comply with any exercise of Data Subject Requests set forth in the applicable Data Protection Laws by a Data Subject or a Supervisory Authority, to the extent Controller does not have the ability to fulfill such a request. Notwithstanding anything to the contrary, Controller shall be solely responsible for complying with the Data Subject Requests and its own obligations under Data Protection Laws.

5. CALIFORNIA-RELATED PROCESSING OF PERSONAL DATA

5.1. The parties acknowledge and agree that with regard to the Processing of Personal Information under California Data Protection Laws, JFrog is the Service Provider and Customer is the Business.

5.2. In connection with the provision of the JFrog Platform to the Customer, if California Data Protection Laws apply and to the extent JFrog Processes Personal Data on behalf of Customer, JFrog may (i) not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise share Personal Data to any third party for monetary compensation; (ii) not use Personal Data provided by Customer in connection with the Agreement to identify or contact Data Subjects for behavioral advertising or retargeting outside the Permitted Purpose or the direct business relationship with the Customer, unless obtained directly by JFrog; and (iii) combine Personal Data with data received from other entities to the extent necessary to detect Security Breach or protect against fraudulent or illegal activity.

5.3. Customer hereby approves and consents to the use and transfer of Personal Data by JFrog to its applicable Affiliates, service providers, third parties and vendors, in order to provide the JFrog Platform to Customer.

5.4. To exercise Data Subject Rights under California Data Protection Laws, Customer may email JFrog at privacy@jfrog.com; or call JFrog at +1-408-329-1540.

6. RESTRICTED TRANSFERS

6.1. With respect to Restricted Transfers of Personal Data that is protected by the GDPR or the UK GDPR as applicable, the Parties hereby enter into the EU SCCs, completed as set out below in **Appendix 2** of this DPA, which shall also be deemed amended as specified by the UK Addendum.

6.2. Both Parties have the authority to enter into the SCCs for themselves and their respective relevant Affiliates. If the mechanism for Restricted Transfers of Personal Data outside of the EEA and/or the UK changes or requires an update, JFrog will put in place alternative arrangements for such Restricted Transfers, as required by applicable Data Protection Laws.

7. SECURITY RESPONSIBILITIES

7.1. JFrog shall ensure an appropriate level of security, considering the state of the art, the costs of implementation, the nature, scope, context, and the Permitted Purpose of the Processing, as well as the severity of the risk, and industry best practices, when implementing and maintaining the TOMs described in **Appendix 3**.

7.2. JFrog shall regularly monitor compliance with the TOMs and will ensure that JFrog's information security policies and procedures coincide with the organizational controls intended to meet the JFrog Certificate Program.

7.3. Controller acknowledges that the TOMs may be updated from time to time to reflect process improvements or changing practices, provided that the modifications shall not materially decrease the overall security of the JFrog Platform during the term of the Agreement.

8. SECURITY BREACH

8.1. Upon becoming aware of a Security Breach involving Personal Data, JFrog will notify Controller without undue delay and within seventy-two (72) hours, unless such notification is delayed or prohibited by applicable law. To the extent possible, JFrog will provide the Controller with a description of (i) the nature of the Security Breach; (ii) likely consequences of the Security Breach; and (iii) mitigation measures taken to address the Security Breach.

8.2. JFrog shall take all necessary steps consistent with industry best practices, considering the severity of the risk, to resolve such Security Breach as quickly as possible and to prevent its recurrence. JFrog will reasonably assist the Controller with conducting investigations and analysis regarding the Security Breach.

8.3. The Controller is responsible for complying with Security Breach notification laws applicable to Controller and fulfilling any third-party notification obligations related to the Security Breach. JFrog will cooperate with Controller, to the extent reasonably requested, in relation to any notifications to Supervisory Authorities or to affected Data Subjects which are required following a Security Breach, insofar as it relates to JFrog's Processing of Personal Data under this DPA.

8.4. JFrog's notification of or response to a Security Breach will not be construed as an acknowledgement by JFrog of any fault or liability with respect to the Security Breach. To the extent legally permissible, Controller will not communicate any findings or admission of liability concerning any Security Breach which directly or indirectly identifies JFrog without JFrog's prior written approval.

9. SUB-PROCESSORS

9.1. JFrog may engage third-party service providers to Process Personal Data on behalf of Controller ("**Sub-Processors**") for the duration of the Agreement. Controller provides JFrog with a general authorization to engage the Sub-Processors listed at **Appendix 4** below. JFrog may engage with a new Sub-Processor to Process Personal Data on Controller's behalf. JFrog shall maintain a list of Sub-Processors available online, and Controller shall subscribe to notifications of new Sub-Processors at https://jfrog.com/trust/privacy/sub-processors/. When Controller subscribes, JFrog will provide notification of a new Sub-Processor thirty (30) days before permitting them to Process Personal Data in connection with the provision of the JFrog Platform. All Sub-Processors are required to abide by substantially equivalent obligations as JFrog under this DPA as applicable to their performance of the related service. JFrog shall be responsible for its Sub-Processors' compliance with the obligations of this DPA.

9.2. Controller may object to JFrog's use of a new Sub-Processor for reasonable data protection concerns, relating to the protection of Personal Data intended to be Processed by such Sub-Processor, by notifying JFrog in writing to privacy@jfrog.com within ten (10) days following JFrog's notification. If no objection is received, it is deemed the Controller has authorized the intended changes. In the event Controller objects to such new Sub-Processor, JFrog will use reasonable efforts to make available and/or recommend a commercially reasonable change to the configuration or use of the JFrog Platform by the Controller to avoid Processing of Personal Data by the objected new Sub-Processor without unreasonably burdening the Controller. If within ninety (90) days from Controller's reasonable objection, JFrog is not able to provide a commercially reasonable alternative, Controller, as its sole and exclusive remedy in connection therewith, may terminate the affected Processing of Personal Data on thirty (30) days prior written notice to JFrog.

10. AUDIT REPORTS

10.1. Controller may assess JFrog compliance with this DPA subject to: (i) prior written request of at least thirty (30) days; (ii) once a year; and (iii) valid confidentiality obligations.

10.2. JFrog will provide Controller and any mutually authorized third-party representative with applicable documentation relating to the protection of Personal Data in the form of (a) privacy and information security questionnaires; and (b) copies or extracts from JFrog's relevant audits, reviews, tests, or certifications (collectively "**Audit Reports**"), in accordance with the JFrog Certificate Program.

10.3. Controller acknowledges that JFrog Certificate Program is audited annually by independent third-party auditors. If the requested audit scope is addressed in the JFrog Certificate Program, the Controller agrees to accept the findings presented in the Audit Reports in lieu of requesting an audit of the same controls.

10.4. JFrog shall not be required to provide information that may cause JFrog to compromise its own internal, legal, or regulatory compliance obligations or that is commercially sensitive.

11. DATA PROTECTION IMPACT ASSESSMENT

Considering the nature of the Processing and the information available to JFrog, JFrog will, when required by Data Protection Laws, assist Controller with its obligations related to data protection impact assessments, and prior consultation with Supervisory Authorities, only to the extent that Controller does not otherwise have access to the relevant information, including by providing the information outlined in Section 10 above (Audit Reports).

12. GOVERNMENT REQUESTS

Upon receipt of any request for disclosure of Personal Data by any government, including governmental bodies and law enforcement agencies, JFrog shall, to the extent allowed by law, (i) promptly forward and notify the Controller of receipt of such request; (ii) make reasonable efforts to oppose the request if possible; and (iii) limit the scope of any disclosure to what is strictly necessary to respond to the request.

13. DELETION OF PERSONAL DATA

Upon termination or expiration of the Agreement, JFrog shall delete Personal Data provided by the Controller pursuant to the Agreement, within sixty (60) days, except: (i) as required by applicable law; (ii) to fulfill legal obligations; (iii) to protect JFrog's legal rights; and (iv) as stored in JFrog's backup system, provided that such Personal Data shall continue to be subject to the provisions of this DPA. In such case the relevant Personal Data shall be securely isolated and protected from any further Processing, except to the extent required by applicable law. JFrog will not have any obligation to retain Personal Data following the termination of the Agreement.

14. CONFLICT

In the event of any conflict or inconsistency between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data. In the event of any conflict between certain provisions of this DPA and any of its Schedules and the SCCs, the latter shall prevail.

15. GOVERNING LAW AND JURISDICTION

Without prejudice to clauses 17 and 18 of the SCCs, this DPA and all non-contractual or other obligations arising out of or in connection with it, are governed by the laws and subject to the exclusive jurisdiction of the courts set out in the Agreement.

16. MODIFICATIONS

Each Party may, by at least forty-five (45) days prior written notice to the other Party, request in writing variations to this DPA if they are required as a result of any change in applicable Data Protection Laws, to allow Processing of such Personal Data to be made (or continue to be made) without breach of applicable Data Protection Laws. Pursuant to such notice, the Parties shall use commercially reasonable efforts and negotiate in good faith to accommodate such required modifications as soon as is reasonably practicable. In addition, JFrog may amend this DPA from time to time without notice, provided that such changes are not adverse in any material aspect with respect to the Controller's rights or JFrog's obligations. If JFrog shall make such material adverse changes, JFrog will notify Controller by posting an announcement on the Website, via the JFrog Platform and/or by sending an email.

APPENDIX 1: DETAILS OF PROCESSING

Nature and Purpose of Processing	Providing the JFrog Platform to the Controller.
Categories of Data Subjects	Controllers' employees authorized to use the JFrog Platform.
Types of Personal Data	Username, email address and IP address.
Special Categories of Personal Data transferred	Not applicable.
Duration of Processing	For the duration of the Agreement, and subject to local legal requirements.
Frequency of transfer	Continuous basis for the duration of the Agreement.
For transfers to Sub-Processors	As described above.

APPENDIX 2: STANDARD CONTRACTUAL CLAUSES

The Parties agree that the terms of Module II – Controller to Processor of the EU SCCs (available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), together with the UK Addendum (available at: https://ico.org.uk/media/about-the-ico/consultations/2620398/draft-ico-addendum-to-com-scc-20210805.pdf) are hereby incorporated by reference and shall apply to a Restricted Transfer, as follows:

Clause 7 *Docking Clause*	Shall not apply.	
Clause 9(a) *Use of Sub-Processors*	Option 2: general written authorization shall apply; prior notification, the method for appointing and objecting to such changes shall be as set forth in Section 9 of this DPA.	
Clause 11 *Redress*	The optional language shall not apply.	
Clause 17 *Governing law*	Option 1 shall apply; the Parties agree that the EU SCCs shall be governed by the laws of the Republic of Ireland; the UK Addendum shall be governed by the laws of England and Wales.	
Clause 18(b) *Jurisdiction*	Disputes will be resolved in the EU before the courts of the Republic of Ireland, and in the UK before the courts of England and Wales.	
Annex I.A *List of Parties*	*Customer / data exporter*	*JFrog / data importer*
	Controller	Processor
	Use of the JFrog Platform	Provision of the JFrog Platform
	Name, address and contact details are detailed in the Agreement.	
	By entering into the Agreement and/or DPA, data exporter is deemed to have signed these SCCs incorporated herein, including their Annexes, as of the Effective Date of the Agreement.	
Annex I.B *Description of Transfer*	As detailed in Appendix 1 of this DPA.	
Annex I.C *Supervisory Authority*	EEA - will be determined in accordance with the GDPR. UK - ICO	
Annex II *TOMs*	As detailed in Appendix 3 of this DPA.	
Annex III *Sub-Processors List*	As detailed in Appendix 4 of this DPA.	

APPENDIX 3: TECHNICAL AND ORGANIZATIONAL MEASURES

Access Control	● Each cloud Customer account is: (i) deployed with a unique ID to guarantee adequate separation; (ii) granted with its own unique and narrow role, based on least privilege principle. Permissions are granted as required to perform tasks and access shared resources, such as databases and cloud object storage. ● The default and automatic deployment of the JFrog Platform is on a shared environment including the following resources: o The load balancer is a shared component at the region level; o The applications' database schema and role are dedicated for each Customer; o The applications' database and file store are deployed using a cloud provider managed service, shared at the region level; o Each Customer has its own unique role with permissions for their own files. ● JFrog Platform uses managed object storage and databases from the major cloud providers.
Data Encryption	● Data in transit is defined as data that is actively transferring between different destinations (e.g., applications to databases or object storage) over the same network or over the internet. In the JFrog Platform Customer Data is encrypted in transit using HTTPS with TLS V1.2. ● Data at rest is defined as data that is physically stored and hosted in any digital form (e.g., cloud storage, databases, data warehouses, or cloud backups) and not actively transferring between different destinations. In the JFrog Platform, all hosted data at rest is securely stored in a database and object storage using 256-bit AES encryption.
Application and Infrastructure Control	● As part of our multi-layer cloud protection approach, a dedicated DDoS mitigation ecosystem has been put in place. JFrog utilizes anti-DDoS protection, a next-gen WAF, an API protection tool, advanced rate limiting and bot protection. ● JFrog's Cyber Incident Response Team (**CIRT**) constantly monitors our products, infrastructure operations and security solutions. JFrog's security has established a comprehensive strategy and policies to respond, notify, and remediate security incidents promptly and efficiently. ● JFrog's CIRT continuously monitors our products' logs, infrastructure operations and systems audit logs in our internal Security Information and Event Management (**SIEM**) to detect potential incidents promptly and efficiently. As part of this ongoing effort, the CIRT investigates and responds to reports from bug bounty programs, vulnerability disclosure programs, automated scanners, Customer support portal and dedicated email inbox. ● To ensure prompt and efficient response time, our Security Operations Center (**SOC**) is staffed with highly qualified and experienced security experts, who work to fulfill our internal SLA policy.
Network Control	JFrog has appropriate network perimeter defense solutions in place, to monitor, detect, and prevent malicious network activity and restrict access to authorized users and services.
Internal Controls	● JFrog has defined access roles for each system and service based on least privilege principle. Access to all our applications is possible only via Single Sign-on (**SSO**) and 2-factor authentication (**2FA**) with strong password policies. ● JFrog requires that its employees use a password manager to ensure that they use unique and complex passwords and store them in a secure vault.

	● JFrog uses a zero-trust solution to securely connect our employees, devices, and apps over JFrog's internal network. Our zero-trust solution provides Web and URL filtering, sandboxing, cloud firewall, CASB and DLP. ● JFrog engineers connect to our production resources using an advanced 2FA and just-in-time access solution, which allows us to employ the principle of least privilege and conduct a full audit. ● JFrog laptops are equipped with encryption technology that is turned on by default, along with advanced anti-malware software. ● JFrog uses email protection solutions designed to prevent malware, zero-day attacks, phishing, Business Email Compromise (**BEC**), spam and N-days. ● JFrog employees receive mandatory data protection and cyber security awareness training as part of their onboarding, as well as ongoing training thereafter. Moreover, employees receive ongoing security education training about topics such as phishing, password management, secure development, and security best practices for operating cloud accounts.
Backup	JFrog maintains an internal backup solution for the Artifactory instance, by replicating the storage and database to a different region in the same continent. For the removal of doubt, the purpose of such backup is solely to ensure JFrog's continuous ability to provide use of the JFrog Platform and is not intended for the restoration of Customer Data upon Customer request.
Business Continuity Plan and Disaster Recovery Plan	JFrog maintains a Business Continuity Plan (**BCP**) and a Disaster Recovery Plan (**DRP**) consistent with industry best practices for the JFrog Platform, which is tested annually. In addition, the BCP and DRP will ensure: (i) installed systems used to provide the JFrog Platform will be restored in case of interruption; (ii) JFrog's ability to restore the availability and access to the Customer Data in a timely manner in the event of a physical or technical incident; and (iii) the ongoing confidentiality, integrity, availability, and resilience of systems JFrog uses to provide the JFrog Platform.
Security Events	JFrog's CIRT works with external incident response experts to assist JFrog with emergency security incidents. As part of JFrog's comprehensive vulnerability management process, JFrog's CIRT runs continuous and automated vulnerability scans of all our assets; prioritizes vulnerability fixes and releases patches quickly.
Certificate Program	● JFrog is certified under **ISO 27001**, the global standard for IT security management policies. ISO 27001 is a framework of policies and procedures that includes people, processes, and IT systems, its objective is to provide requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). ● JFrog is certified under **ISO 27701**, the data privacy extension to ISO 27001/2. This Privacy Information Management System (PIMS) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage privacy controls and to reduce the risk to the privacy rights of individuals. ● JFrog is certified under **ISO 27017**, the global security standard for cloud service providers and users. ISO 27017 provides guidance on the information security aspects of cloud computing, to make a safer cloud-based environment and reduce the risk of security issues. ● JFrog engages Ernst & Young to audit its System and Organization Controls Report - **SOC 2 Type II Report**. This auditing procedure ensures we securely manage and protect our Customer's data. This Report is validated and updated annually and is a key document that outlines and certifies the ways in which JFrog achieves and maintains compliance and control objectives.

APPENDIX 4: SUB-PROCESSORS AND AFFILIATES LIST

Sub-Processors

Used to host Customer Data as chosen by the Customer

Name	Purpose / Location	Contact	TOMs
Amazon Web Services, Inc. (AWS)	Cloud Computing Services. Controllers can choose the location and region in accordance with the list available here: https://status.jfrog.io/.	https://aws.amazon.com/contact-us/compliance-support/	https://aws.amazon.com/compliance/programs/
Google Cloud Platform, LLC (GCP)		https://support.google.com/cloud/contact/dpo	https://cloud.google.com/security/compliance/offerings
Microsoft Azure, Corp. (Azure)		https://www.microsoft.com/en-us/concern/privacy	https://learn.microsoft.com/en-us/azure/compliance/

Used to provide specific functionality within the JFrog Platform

Name	Purpose / Location	Contact	TOMs
Amazon Web Services, Inc. (AWS)	Logs cloud hosting services. United States.	https://aws.amazon.com/contact-us/compliance-support/	https://aws.amazon.com/compliance/programs/
Coralogix, Inc.	Log aggregation and correlation services. United States.	legal@coralogix.com	https://coralogix.com/security-and-compliance/
Mailgun Technologies, Inc.	Email notification services. United States.	https://www.mailgun.com/contact/support/	https://www.mailgun.com/security/
SendGrid (Twilio, Inc.)	Email notification services. United States.	https://sendgrid.com/contact/	https://sendgrid.com/policies/security/

Affiliates

Used for administrative, billing and support purposes

Name	Type	Location	Address
JFrog Ltd.	Parent Company	Israel	3 HaMachshev Street, Netanya 4250465
JFrog Inc.	Affiliate	United States	270 E Caribbean Dr., Sunnyvale, CA 94089
JFrog Japan KK	Affiliate	Japan	1-9-2 Otemachi, Chiyoda-ku, Tokyo, 100 0004
JFrog India Pvt Ltd.	Affiliate	India	Salarpuria Softzone, Wing 'A', Floor 1, Nos. 80/1, 81/1 and 81/2 Bellandur, Bangalore 560 037