JFROG CLOUD DATA PROCESSING ADDENDUM

This **JFrog Cloud Data Processing Addendum** ("**DPA**"), including all Appendices, forms part of the **JFrog Cloud Terms and Conditions** available at https://jfrog.com/cloud-terms-and-conditions/ or the agreement entered between JFrog and Customer (the "**Agreement**"). In the course of providing services to Customer pursuant to the Agreement, JFrog may process Personal Data on behalf of Customer in connection with the JFrog Platform, the provisions of this DPA will apply.

1. DEFINITIONS

Any capitalized terms which are not defined herein, shall have the meaning provided to them in the Agreement. In this DPA, the following terms will have the meanings set out below:

1.1. **"Business"**, "**Controller**", "**Member State**", "**Processes**" "**Processing**", "**Processor**", "**Sell**", "**Service Provider**", "**Share**", "**Special Categories of Personal Data**", and "**Supervisory Authority**" and their derivatives shall have the same meaning as defined in Data Protection Laws and may be lowercase or uppercase herein;

1.2. "**Data Protection Laws**" means data protection laws and regulations applicable to JFrog's processing of Personal Data to provide the services, including (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**"); (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**"); and (iv) Swiss Federal Act on Data Protection which means the revised FADP version of 25 September 2020, **("FADP")**, as amended, or superseded from time to time, and as applicable to the Processing of Personal Data under this DPA;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 in its role as a Processor on behalf of Customer under this DPA and the Agreement;

1.5. **"EU SCCs"** means the standard contractual clauses for the transfer of Personal Data to Controllers and Processors established in third countries, adopted by the European Commission from time to time, the adopted version in force at the date of signature of this DPA and set out in Implementing Decision (EU) 2021/914 of 4 June 2021 found at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj; and

1.6. **"UK Addendum"** means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses found at https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf, as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

2. ROLES OF THE PARTIES; DETAILS OF PROCESSING

The Parties acknowledge and agree that the Processing of Personal Data by JFrog is for the provision of the JFrog Platform pursuant to the Agreement. The Parties agree Customer is the Controller and Business and JFrog is the Processor and Service Provider. JFrog will Process such Personal Data until the expiration or termination of the Agreement unless otherwise instructed in writing by Customer. 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**. Each Party will comply with its respective obligations under the Data Protection Laws.

3. DISCLOSING OF PERSONAL DATA

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

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

3.3. Customer has the sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

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

3.5. Customer will only disclose Personal Data necessary for the performance of the services and will not disclose any Special Categories of Personal Data to JFrog.

4. PROCESSING OF PERSONAL DATA

4.1. JFrog will only Process Personal Data on behalf of and in accordance with Customer's reasonable instructions as detailed in this DPA and within Customer's configuration of the services for the purpose of providing the Services to Customer, or as otherwise required by applicable law.

4.2. JFrog will inform Customer without undue delay if, in JFrog's opinion, any Customer instructions infringe Data Protection Laws. JFrog is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation.

4.3. JFrog will 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.

4.4. JFrog will 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 or are under an appropriate statutory obligation of confidentiality and received appropriate information security and privacy training on their responsibilities.

4.5. JFrog will maintain appropriate Technical and Organizational Measures as provided in the JFrog Cloud Data Security Addendum (**Appendix 2**) to protect Personal Data against a Security Incident and taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons provided in **Appendix 1**. Regarding a Security Incident involving Personal Data the general provision on Security Incidents in the Agreement will apply.

4.6. JFrog will reasonably assist Customer with Customer's compliance obligations regarding Personal Data Security Incidents, data protection impact assessments, Data Subject Requests, and prior consultation, each as and to the extent required by Data Protection Laws, taking into account the nature of Processing and the information available to JFrog. In the event JFrog receives a Data Subject Request regarding JFrog processing of Personal Data on behalf of Customer, JFrog will only respond to the Data Subject to acknowledge receipt, identify the Customer, and acknowledge that the Customer will respond to the Data Subject directly or as required by Data Protection Laws.

4.7. JFrog is not responsible for determining the requirements of laws or regulations applicable to Customer's business, or that the Service meets the requirements of any such laws or regulations.

4.8. If California Data Protection Laws apply and to the extent JFrog Processes Personal Data on

behalf of Customer subject to the CCPA, JFrog may not:
(i) Sell or Share Personal Data as defined within the CCPA;
(ii) retain, use, or disclose Personal Data outside of the direct business relationship between JFrog and Customer;
(iii) 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 Customer, unless obtained directly by JFrog; and
(iv) combine Personal Data that JFrog receives from Customer with Personal Data JFrog receives from, or on behalf of, another person, or collects from its own interaction with Data Subjects, except where both expressly required to perform the services and permitted by Data Protection Laws.

5. TRANSFERS OF PERSONAL DATA

5.1. For transfers of Customer Personal Data from the EEA, UK and Switzerland to countries in which JFrog, as a data importer, is located there are adequacy decisions from the European Commission and corresponding agreements for the UK and Switzerland, on the basis of which this transfer of data is permissible. In the event that these adequacy decisions become ineffective, we agree on the following as a subsidiary transfer mechanism:

5.1.1. Clause 7: The optional docking clause will not apply.

5.1.2. Clause 9(a): Option 2: General written authorization shall apply and the time period is set forth in the Sub-Processor section in this DPA.

5.1.3. Clause 11: The optional language will not apply.

5.1.4. Clause 17: Option 1: The Parties agree that the EU SCCs will be governed by the laws of the Republic of Ireland.

5.1.5. Clause 18(b): Disputes will be resolved in the EU before the courts of the Republic of Ireland.

5.1.6. Annex I.A and I.B: Completed with information set out in **Appendix 1**.

5.1.7. Annex IC: Where Customer is established in the EEA, the supervisory authority with responsibility for ensuring data transfer compliance by Customer with GDPR will act as competent supervisory authority. Where Customer is not established in the EEA, but is within the territorial scope of application of GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1), the supervisory authority will be the member state the Article 27(1) representative is established. If Customer is not established in the EEA, but falls within the territorial scope of GDPR without having to appoint a representative, the Commission nationale de l'informatique et des libertés (CNIL) will act as the competent authority.

5.2. Annex 2: Technical and organizational measures completed with information set out in Appendix 2. Both Parties have the authority to enter into the EU SCCs for themselves and their respective relevant Affiliates. If the mechanism for transfers of Personal Data requires an update, JFrog will put in place alternative arrangements for such transfers, as required by Data Protection Laws. For avoidance of doubt, signature on this DPA will be deemed to constitute a signature on the EU SCCs.

5.3. Where the UK Addendum applies, it is hereby incorporated by reference and completed as follows:

5.3.1. Tables 1, 2, and 3 are completed with the relevant information from the EU SCCs completed in section 5.1 and **Appendix 1** in this DPA. Table 4, the option of neither party is selected.

5.3.2. Where Customer is established in the U.K. or falls within the territorial scope of application of the UK Data Protection Laws and Regulations, the Information Commissioner's Office (ICO) will act as competent supervisory authority.

5.4. Where Personal Data is subject to the Switzerland FADP, the EU SCCs will apply with the following modifications:

5.4.1. Any references to Directive 95/46/EC, Regulation (EU) 2016/679 or GDPR are interpreted as references to FADP. References to EU, Union, Member State Law will have the same meaning as the equivalent reference in the FADP.

5.4.2. Where Customer is established in Switzerland or falls within territorial scope of the FADP, the Swiss Federal Data Protection and Information Commissioner will act as competent supervisory authority insofar as the relevant data transfer is governed by the FADP.

5.5. JFrog, Inc. has certified to participate in and comply with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively the "DPF") and the commitments they entail, as detailed at www.dataprivacyframework.gov.

6. SUB-PROCESSORS

6.1. Customer grants JFrog general authorization to engage and use third parties to fulfill its contractual obligations to Process Customer Personal Data under the Agreement ("**Sub-Processors**"). JFrog shall maintain a list of Sub-Processors available online, and Customer shall subscribe to notifications of new Sub-Processors at https://jfrog.com/trust/privacy/sub-processors/.

6.2. JFrog will provide Customer with thirty (30) day notice ("**Notice Period**") prior to adding or replacing any Sub-Processor by posting details at https://jfrog.com/trust/privacy/sub-processors/. Customer may object to JFrog's use of the new or replacement Sub-Processor due to reasonable data protection concerns relating to the particular Personal Data intended to be Processed by such Sub-Processor, Customer will provide JFrog written notice of its objection and its reasonable data protection grounds at privacy@jfrog.com within the Notice Period. In the event Customer objects to the 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 Customer to avoid Processing of Personal Data by the objected new Sub-Processor without unreasonably burdening Customer. If within ninety (90) days from Customer's reasonable objection, JFrog is not able to provide a commercially reasonable alternative, Customer, 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.

6.3. If Customer does not object within the Notice Period, the respective Sub-Processor will be commissioned to Process Personal Data. Sub-Processors are required to abide by substantially equivalent obligations as JFrog under this DPA as applicable to their performance of the related service and JFrog will remain responsible to Customer for JFrog's Sub-Processors that cause JFrog to breach any of its obligations under this DPA.

7. AUDIT REPORTS

Customer 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. JFrog will provide Customer 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 located at https://jfrog.com/trust/certificate-program/ ("**JFrog Certificate Program**"). Customer acknowledges that the JFrog Certificate Program is audited annually by independent third-party auditors. If the requested audit scope is addressed in the JFrog Certificate Program, Customer agrees to accept the findings presented in the Audit Reports in lieu of requesting an audit of the same controls. JFrog will 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.

8. GOVERNMENT REQUESTS

Upon receipt of any request for disclosure of Personal Data by any government, including governmental bodies and law enforcement agencies, JFrog will promptly direct the government requestor to the Customer. If redirection is not possible, JFrog will notify Customer, unless legally prohibited from doing so. In such case, JFrog will take reasonable steps to notify Customer after the nondisclosure requirement expires. JFrog will not provide Personal Data in a bulk or indiscriminate manner. JFrog will only disclose Personal Data to the extent JFrog is legally required to do so and only in accordance with applicable lawful process.

9. DELETION OF PERSONAL DATA

Upon termination or expiration of the Agreement, JFrog shall delete Personal Data provided by the Customer 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.

10. CONFLICT; REMEDIES

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 Appendices and the EU SCCs, the latter shall prevail. This DPA will be subject to the Limitation of Liability and Indemnification provisions agreed upon between the Parties set forth in the Agreement. This section will not be construed to limit the liability of either Party with respect to claims brought under EU SCC Clause 12, the UK Addendum, or by Data Subjects. Nothing in this DPA is intended to contradict the applicable terms in the Data Protection Laws, the EU SCCs, or the UK Addendum.

11. GOVERNING LAW AND JURISDICTION

Without prejudice to clauses 17 and 18 of the EU 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.

12. MODIFICATIONS

JFrog may amend this DPA from time to time as a result of changes in Data Protection Laws, a merger, acquisition, or similar occurrence, provided that such changes are not adverse in any material aspect with respect to the Customer's rights or JFrog's obligations. JFrog will provide advance notice of an amendment by posting an announcement on the JFrog website, via the JFrog Platform, or by sending an email. By continuing to use the services after the effective date of any amendments to this DPA, Customer agrees to be bound by the modified DPA.

IN WITNESS WHEREOF, the Parties below have executed this legally binding DPA, executed by their duly authorized representatives as of the last date of execution below ("**Effective Date**").

JFrog	**Customer**
Name:	Name:
Title:	Title:
Date:	Date:
By:	By:

The rest of this page is intentionally blank.

APPENDIX 1: DETAILS OF PROCESSING

Data Exporter, Role and Contact Details:	Customer - Controller - As set out in this DPA.
Data Importer, Role and Contact Details:	JFrog - Processor - As set out in this DPA.
Nature and Purpose of Processing:	Providing the JFrog Platform to the Customer.
Categories of Data Subjects:	Customers' Users authorized to use the JFrog Platform.
Types of Personal Data:	Username, name, title, email address and IP address and all information associated with these identifiers.
Special Categories of Personal Data Transferred:	Not applicable.
Duration of Processing:	For the duration of the Agreement, and subject to legal requirements.
Frequency of Transfer:	Continuous basis for the duration of the Agreement.
Personal Data Retention:	Provided in the Deletion of Personal Data section of this DPA.
For Transfers to Sub-Processors:	Provided in the Sub-Processors section of this DPA.

APPENDIX 2: JFROG CLOUD DATA SECURITY ADDENDUM

This JFrog Cloud Data Security Addendum ("**DSA**" or "**TOMs**") describes the technical and organizational security measures (TOMs) that JFrog maintains to protect Customer Data (including Personal Data, as applicable) and Confidential Information. JFrog reserves the right to update the DSA, at its sole discretion, where updates will not materially degrade the security protocols or security levels in place as of the Effective Date during the applicable Subscription Term. Changes will be reflected at https://jfrog.com/jfrog-toms/. This DSA forms part of the JFrog Agreement between JFrog and Customer and applies to Self-Hosted Subscriptions as applicable. Any capitalized terms which are not defined herein, shall have the meaning provided to them in the Agreement or the DPA.

1. JFrog Security Program

JFrog has implemented and maintains appropriate administrative, technical, physical, and organizational measures to ensure a level of security appropriate to the level of risk, in accordance with industry standards. JFrog maintains security policies, standards, and controls related to security, confidentiality, integrity, and availability. These policies are reviewed and approved annually and updated as needed.

2. Certificate Program / Security Certifications

JFrog maintains the following certifications and governance methods:

(a) Certification under ISO/IEC 27001:2013, ISO/IEC 27701:2019, ISO 27017:2014, and SOC 2, Type 2.

(b) Annual security audits by an independent third party, covering security, confidentiality, and availability control criteria.

(c) Regularly tests and monitors the effectiveness of its information security program through internal audits aligned with the relevant compliance controls and frameworks. Issues identified are documented, tracked, and remediated as appropriate.

3. Access and Authentication Controls

JFrog has implemented and maintains the following measures:

(a) Access Control Policy in accordance with the "least privileges" and "need to know" principles.

(b) Strict role-based permissions are granted in accordance with the role requirements.

(c) Access permissions are reviewed on a regular basis. Any access which is inappropriate for a role function is promptly removed.

(d) Access to JFrog systems and networks are disabled promptly upon notification in the event of termination of personnel.

(e) Unique usernames and passwords with minimum length and complexity requirements are enforced for all users.

(f) Two-factor authentication (2FA) is required for remote access and privileged account access.

(g) Physical access to JFrog facilities is restricted and requires a key-card, access is logged and maintained. Visitors are accompanied at all times and confidentiality measures are in place. Additional measures include video surveillance and other industry-standard practices.

(h) Services operate on a multitenant architecture designed to segregate and restrict access to Customer Data hosted on the JFrog platform. JFrog architecture provides a logical data separation for each different Customer via a unique ID.

4. HR, Security, Training and Awareness

JFrog has implemented and maintains the following measures:

(a) Background checks are conducted commensurate with job duties, in accordance with applicable laws and regulations.

(b) Personnel are subjected to non-disclosure or confidentiality obligations.

(c) Personnel are required to complete security awareness and privacy training during onboarding and at least annually thereafter.
(d) Personnel are required to review and acknowledge security policies during onboarding and annually thereafter.
(e) Periodic security and privacy awareness campaigns aimed to further educate personnel about their responsibilities.

5. Risk Management and Infrastructure Control

JFrog has implemented and maintains the following measures:

(a) JFrog Management reviews documented risks to determine appropriate risk levels and treatment options.
(b) Encryption and Key Management: Industry-standard encryption techniques (TLS 1.2 for data in transit and 256-bit AES for data at rest). Encryption keys are managed in a cloud-hosted key management service (KMS).
(c) Threat and Vulnerability Management: Continuous monitoring, annual penetration tests, and ongoing vulnerability scans are performed to identify and remediate potential threats. Patches are applied regularly after testing for safety. Vulnerabilities are classified based on the Common Vulnerability Scoring System (CVSS), a remediation plan is developed, including the steps required to address the vulnerability and the timeline for completion based on the remediation time for each severity level.
(d) Logging and Monitoring: Monitoring tools and services are used to monitor systems for various events. Logs are stored securely and reviewed by the security team utilizing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) technology.
(e) Network Security: Zero-Trust Security Technology to prevent unauthorized access to JFrog networks, servers, or applications.
(f) Cloud Security: Utilization of cloud provider-managed DDoS mitigation services, next-generation Web Application Firewall (WAF), API protection, advanced rate limiting, and bot protection. These measures are designed to safeguard against various types of cyber threats. Regular cloud security scanning tools are employed, including advanced Cloud Security Posture Management (CSPM) solutions, to enforce security best practices and mitigate potential misconfigurations.
(g) Development Security: Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, and management of software components. JFrog follows OWASP (Open Web Application Security Project) guidelines to ensure that security is integrated throughout the development process.
(h) Infrastructure as Code: Infrastructure as Code (IaC) serves as a critical component aligning DevOps, Security, and compliance efforts within JFrog's operational framework. This approach ensures secure management of infrastructure processes by automating and standardizing deployments. JFrog’s application images undergo rigorous hardening using secured base images and deployment configurations. Continuous security scanning through JFrog’s Xray during the CI build process further enhances security measures.

6. Incident Response

JFrog maintains an Incident Response Plan and computer incident response team (CIRT) to respond to Security Incidents. The plan is reviewed at least annually. Affected Customers will be notified in accordance with the applicable Security Incident section in the Agreement or DPA.

7. Third-Party Risk Management

JFrog has implemented and maintains the following measures:

(a) JFrog conducts security due diligence and risk assessments of Third Parties.

(b) Periodic audits validate the ongoing governance of control operations and risk.
(c) Security controls and obligations are incorporated into Third Party contracts.
(d) Data Center Security: JFrog Data Centers are hosted by Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) which offer robust data center security measures. These include physical security with 24/7 staff and access control, advanced environmental controls, extensive network security, and compliance with standards like ISO/IEC 27001:2013 and SOC 2 Type II. Data centers are designed for high availability with redundancy and failover capabilities, and data is encrypted both at rest and in transit to ensure protection against unauthorized access.

8. Customer Security Considerations

Customers are responsible for their own security measures, including secure password practices, user management, timely software updates (outside of JFrog cloud), and proper access controls. JFrog is not liable for security incidents or data losses resulting from client-side vulnerabilities. JFrog maintains an inventory of infrastructure assets and has documented data disposal policies. Customer Data will be securely deleted as referenced in the Agreement.

9. Contingency Planning

JFrog has implemented and maintains the following measures:

(a) A Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), which are reviewed annually, to manage significant disruptions.
(b) Data backup, replication, and recovery systems are deployed to support resilience.
(c) Annual Disaster Recovery drills are conducted to test and validate JFrog recovery procedures.

APPENDIX 3: 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/

If AI features are enabled within the JFrog Platform:

Name	Purpose/Location	Contact	TOMs
Amazon	Application AI Functionality United States	Contact Amazon AWS	Amazon AWS AI Trust
Google		Contact Google	Google Gemini Privacy Center
Microsoft		Contact Azure	Azure Compliance
Anthropic		Contact Anthropic	Anthropic Trust Center
Meta		Contact Meta	Meta TOMs

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
JFrog Singapore Pte. Ltd.	Affiliate	Singapore	10 Anson Road, #06-17, International Plaza, Singapore 079903