JFROG CLOUD CUSTOMER DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**" or "**Addendum**") is hereby incorporated by reference into, and becomes a binding part of the Terms of Service for JFrog's Cloud Services (the "**Cloud Services**") available at https://jfrog.com/jfrog-cloud-general-terms/, or any other existing agreement between the Customer and JFrog for the provision by JFrog of any of its Cloud Services (the "**Agreement**") in which JFrog and its Affiliates ("**JFrog**" or "**Processor**") act as a Processor of Customer's personal data. Both Parties shall be referred to as "**Parties**". All capitalized terms not defined herein will have the meaning set forth in the Agreement.

For the purposes of this DPA, the term "**Customer**" or "**Controller**" shall include both the individual using the Cloud Services offered under the applicable Agreement and any legal entity on whose behalf such individual is acting. This DPA sets out the terms that apply with regards to the Processing of Personal Data (as defined below) by JFrog, on behalf of Customer, in the course of providing the Cloud Services to Customer under the Agreement.

1. **Definitions.**

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

1.1 "**Controller**", "**Data Subject**", "**Member State**", "**Process/Processing**", "**Processor**", and "**Special Categories of Personal Data**" will have the same meaning as defined in Data Protection Laws;

1.2 "**Data Protection Laws**" means 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**), as well as the **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**), as applicable to the Processing of Personal Data under the Agreement;

1.3 "**Data Subject Request**" means a request from a Data Subject to exercise any right under Data Protection Laws;

1.4 "**International Data Transfer Addendum**" means Standard Data Protection Clauses issued by the UK Information Commissioner Office ("**ICO**") under S119A(1) of Data Protection Act 2018, to the SCCs, for parties making Restricted Transfers ("**UK Addendum**");

1.5 "**Personal Data**" means any Personal Data that is disclosed by Controller to Processor in the performance of Processor's rights or obligations under the Agreement, to the extent such Personal Data is related to residents of the EEA, or the disclosure of such Personal Data is otherwise subject to Data Protection Laws;

1.6 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Processor on behalf of the Controller;

1.7 "**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**");

1.8 "**Standard Contractual Clauses**" means 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 Regulation (EU) 2016/679 as updated, amended, replaced or superseded from time to time by the European Commission ("**SCC**"); and

1.9 "**Supervisory Authority**" means (i) an independent public authority which is established by a Member State pursuant to the GDPR; and (ii) the ICO in the UK.

2. Disclosing of Personal Data.

Controller will:

2.1 only have Processor Process Personal Data in accordance with the requirements of the applicable Data Protection Laws;

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

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

2.4 ensure that a notice has been made available and will continue to be accessible to the relevant Data Subjects informing them that their Personal Data will be disclosed to the Processor or to a category of third party describing the Processor;

2.5 ensure that it has obtained any necessary consents or authorizations required to permit the Processor to freely Process the Personal Data for the Permitted Purposes;

2.6 not disclose any Special Categories of Personal Data to the Processor; and

2.7 be responsible for the security of any Personal Data in transmission from Controller to Processor.

3. Processing of Personal Data.

In its capacity as a Processor, JFrog will:

3.1 only Process Personal Data on behalf of and in accordance with Controller's reasonable instructions;

3.2 not Process Personal Data in a way that is incompatible with the Permitted Purposes (other than to comply with a requirement of applicable law to which Processor is subject);

3.3 not Process Personal Data for longer than is necessary to carry out the Permitted Purposes (other than to comply with a requirement of applicable law to which Processor is subject);

3.4 ensure that its personnel and Sub-Processors comply with equivalent measures in Processing Controller's Personal Data;

3.5 will make best efforts within industry acceptable standards have in place appropriate technical and organizational security measures to protect the Personal Data against unauthorized or unlawful Processing, or accidental loss or destruction or damage; and

3.6 reasonably assist Controller to facilitate the fulfillment of Controller's obligation to comply with any exercise of rights set forth in the applicable Data Protection Laws by a Data Subject or Supervisory Authority.

4. Details of Processing.

The Parties acknowledge that the Processing of Personal Data by JFrog is for the performance of the Cloud Services pursuant to the Agreement. The nature and purpose of the Processing, as well as the duration of the Processing, the types of Personal Data (which shall not include any Special Categories of Personal Data), and categories of Data Subjects Processed under this DPA are detailed in Appendix 1 to this DPA. The Personal Data is disclosed and transferred for the Permitted Purposes as set forth in the DPA.

5. Restricted Transfers.

5.1 With respect to Restricted Transfers of Personal Data from Controller to JFrog, the Parties hereby enter into module II (Controller to Processor) of the SCCs, which is incorporated into this Addendum as Appendix 3; for Restricted Transfer from the UK, the UK Addendum is incorporated as Appendix 4.

5.2 Controller for itself and its relevant Affiliates are the "**data exporter**" and JFrog and its relevant Affiliates are the "**data importer**", and both Parties have the authority to enter into the SCCs and the UK Addendum for themselves and their respective relevant Affiliates.

6. Personal Data Breach.

6.1 JFrog will notify the Controller without undue delay following any Personal Data Breach involving the Personal Data Processed by JFrog on behalf of the Controller.

6.2 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 Personal Data Breach, insofar as it relates to JFrog's Processing of Personal Data under this DPA.

6.3 Controller will not communicate any finding or admission of liability concerning any Personal Data Breach which directly or indirectly identifies JFrog without JFrog's prior written approval.

7. Security Responsibilities.

JFrog is responsible for implementing and maintaining the technical and organizational measures for the Cloud Services as described in Appendix 2 to this DPA, designed to help secure Controller's Personal Data against unauthorized processing and accidental or unlawful loss, access, or disclosure.

8. Sub-Processors.

8.1 JFrog may engage third-party service providers to Process Personal Data on behalf of Controller ("**Sub-Processors**") for the duration of the Cloud Services. Controller provides JFrog with a general authorization to engage the Sub-Processors listed here. JFrog may engage with a new Sub-Processor to Process Personal Data on Controller's behalf. Controller shall subscribe to notifications of new Sub-Processors for the Cloud Services here:

https://jfrog.com/trust/privacy/. When Controller subscribes, JFrog will provide notification of a new Sub-Processor before permitting them to Process Personal Data in connection with the provision of the Cloud Services. All Sub-Processors are required to abide by substantially equivalent obligations as JFrog under this DPA as applicable to their performance of the service;

8.2 Controller may object to JFrog's use of a new Sub-Processor for reasonable and explained grounds, by notifying JFrog in writing to privacy@jfrog.com within 5 (five) business days following JFrog's notification. In the event Controller will object to a new Sub-Processor, JFrog will use reasonable efforts to make available to the Controller a change in the Cloud Services or recommend a commercially reasonable change to the configuration or use of the Cloud Services 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 part of the Cloud Services on thirty (30) days prior written notice to JFrog.

9. Deletion of Data.

Upon termination or expiration of the Agreement JFrog shall delete, within up to sixty (60) days, all Personal Data provided by the Controller pursuant to the Agreement. For the removal of doubt, JFrog will not have any obligation to retain such data following the termination of this Agreement. This requirement shall not apply (i) to the extent JFrog is required by applicable law to which JFrog is subject, to retain some or all of the Personal Data, and (ii) to archived data on back-up systems (e.g., in the form of audit logs). 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.

10. Audit.

Controller, at its own costs and expenses, shall be permitted to monitor JFrog's compliance with this DPA by performing an annual virtual information security assessment. JFrog will: (i) provide Controller and any mutually authorized third-party representative access to all non-internal documentation necessary to demonstrate compliance with this DPA relating to the protection of Personal Data; which may include response to an information security-related questionnaire, copies of relevant audits, reviews, tests, or certifications of JFrog platform or processes, including an annual SOC2 Type II Report, ISO 27001 and ISO 27017 certifications; (ii) maintain its controls to the level attested to Controller in such assessments.

11. 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.

12. Conflict.

12.1 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;

12.2 In the event of any conflict between certain provisions of this DPA and any of its Schedules and the SCCs, the latter shall prevail.

13. Governing Law and Jurisdiction.

Without prejudice to clauses 17 and 18 of the SCCs and the UK Addendum:

13.1 the Parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it, are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

14. Limitation of Liability.

JFrog and its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement.

IN WITNESS WHEREOF, the named Parties below agree to this legally binding Addendum, executed by their duly authorized representatives.

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

JFROG CLOUD CUSTOMER CCPA ADDENDUM

This California Consumer Privacy Act (**CCPA**) Addendum ("**CCPA Addendum**") is hereby incorporated by reference into, and becomes a binding part of the Terms of Service for JFrog's Cloud Services (the "**Cloud Services**") available at https://jfrog.com/jfrog-cloud-general-terms/, or any other existing agreement between the Customer ("**Customer**" or "**Business**") and JFrog ("**JFrog**" or "**Service Provider**") for the provision by JFrog of any of its Cloud Services (the "**Agreement**"). All capitalized terms not defined herein will have the meaning set forth in the Agreement.

1. Definitions.

For purposes of this CCPA Addendum, the following terms shall mean as follows:

1.1 "**CCPA**" means the California Consumer Privacy Act of 2018.

1.2 "**Business**", "**Consumer**", "**Delete**", "**Personal Information**", "**Process**", "**Request to Delete**", "**Request to Know**", "**Sell**", "**Service Provider**" shall have the meaning set forth in the CCPA.

2. Subject Matter.

This CCPA Addendum applies to the Processing by JFrog of Customer Personal Information in connection with the Agreement and the provision of the Cloud Services to Customer, where such Processing is subject to the provisions of the CCPA, and as stipulated in JFrog Privacy Policy.

3. Customer's Obligations.

Customer shall, in its use of the Cloud Services and provision of Personal Information to JFrog and/or the Cloud Services, comply at all times with the obligations, requirements and laws applicable to Businesses and Customer shall indemnify, hold harmless and defend JFrog and its Affiliates for any breach or violation related thereto.

4. Prohibited Use.

4.1 JFrog shall not Sell Customer's Personal Information. JFrog further agrees not to retain, use, or disclose Personal Information obtained from Customer: (i) outside the direct relationship between Customer and JFrog, and (ii) for any purposes other than for the specific purposes of performing the Cloud Services specified in the Agreement.

4.2 For the avoidance of doubt, Customer hereby approves and consents: (i) to the transfer of Personal Information by JFrog to other Service Provider's entities (including, without limitation, Affiliates and subsidiaries), service providers, third-parties and vendors, in order to provide the Cloud Services to Customer; and (ii) that JFrog will use and process the Personal Information in order to (a) provide the Cloud Services to Customer; (b) for internal use by the Service Provider to build or improve the quality of its services; (c) to detect data security incidents, or protect against fraudulent or illegal activity; and (d) collect and analyze anonymous information.

5. **Deletion of Personal Information.**

Upon Customer's written request, and subject to, and in accordance with the provisions of the CCPA, this CCPA Addendum and applicable laws and requirements, JFrog, as a Service Provider, agrees to promptly Delete Customer Personal Information. If the Service Provider receives a Request to Know or a Request to Delete from a Consumer, Service Provider shall inform the Consumer that the request cannot be acted upon because the request has been sent to a Service Provider. To exercise Customer's rights under the CCPA, Customer can: email JFrog at privacy@jfrog.com; or call JFrog at +1-408-329-1540.

6. **Relationship with Agreement.**

Notwithstanding anything to the contrary in the Agreement and/or in any agreement between the Parties and to the maximum extent permitted by law:

6.1 JFrog's and its Affiliates' liability, taken together in the aggregate, arising out of or related to this CCPA Addendum, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement;

6.2 in no event will JFrog and/or JFrog Affiliates and/or their third-party providers, be liable under, or otherwise in connection with, this CCPA Addendum for: (i) any indirect, exemplary, special, consequential, incidental, or punitive damages; (ii) any loss of profits, business, or anticipated savings; (iii) any loss of, or damage to data, reputation, revenue or goodwill; and/or (iv) the cost of procuring any substitute goods or services; and

6.3 the foregoing exclusions and limitations on liability set forth in this Section shall apply: (i) even if JFrog, JFrog Affiliates or third-party providers, have been advised, or should have been aware, of the possibility of losses or damages; (ii) even if any remedy in this CCPA Addendum fails of its essential purpose; and (iii) regardless of the form, theory or basis of liability (such as, but not limited to, breach of contract or tort).

7. **Duration and Survival.**

This CCPA Addendum will become legally binding upon the date JFrog commences to process Customer's Personal Information which is subject to the CCPA. This CCPA Addendum shall automatically terminate upon the termination or expiration of the Agreement under which the Cloud Services are provided. Section 6 and this Section 7 shall survive the termination or expiration of this CCPA Addendum for any reason. This CCPA Addendum cannot, in principle, be terminated separately to the Agreement, except where the processing of Personal Information ends before the termination of the Agreement, in which case, this CCPA Addendum shall automatically terminate. In any event, upon termination, to the extent required or allowed by applicable law, JFrog may retain one copy of the Personal Information for evidence purposes and/or for the establishment, exercise, or defense of legal claims and/or to comply with applicable laws and regulations.

By entering into the Agreement and/or DPA, data exporter is deemed to have signed this CCPA Addendum incorporated herein, as of the Effective Date of the Agreement.

APPENDIX 1: DETAILS OF PROCESSING

Nature and Purpose of Processing	Providing the Cloud Services to the Customer.
Duration of Processing	For the duration of the Cloud Services, and subject to local legal requirements.
Types of Personal Data	Username, email address and IP address. Details on such data are stipulated further in JFrog Privacy Policy.
Categories of Data Subjects	Controllers' employees authorized to use the Cloud Services.

APPENDIX 2: TECHNICAL AND ORGANIZATIONAL CLOUD SECURITY MEASURES

Access Control	• Each cloud Customer account is deployed with a unique ID to guarantee adequate separation. • Each cloud Customer account is granted with its own unique and narrow role, based on least privilege principle. We grant just the permissions which are required to perform tasks and access shared resources, such as databases and cloud object storage. • The default and automatic deployment of JFrog SaaS solution is on a shared environment including the following resources: ○ The load balancer is a shared component at the region level. ○ The applications' database schema and role are dedicated for each Customer. The applications' database is a cloud provider managed service, shared at the region level. ○ Each Customer has its own unique role with permissions for their own files. The applications' file store is a cloud provider managed service, shared at the region level. • JFrog SaaS solution uses managed object storage and databases from the major cloud providers. Each Customer has their own unique role with permissions to their own data.
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 SaaS solution, every Customer's 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 SaaS solution, 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.
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, in compliance with our policy, 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. • All JFrog employees receive mandatory privacy and cyber security awareness training as part of their onboarding, as well as mandatory annual ones 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.
Security Events	• JFrog’s CIRT works with external incident response experts to assist us with emergency security incidents. As part of our comprehensive vulnerability management process, JFrog’s CIRT runs continuous and automated vulnerability scans of all our assets; prioritizes vulnerability fixes and releases patches quickly.
Standards	• ISO 27001, ISO 27017 • SOC 2 Type II

APPENDIX 3: STANDARD CONTRACTUAL CLAUSES

The Parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to a Restricted Transfer, as follows:

Module II – Controller to Processor

Clause 7 - Docking Clause	Shall not apply.
Clause 9(a) - Use of Sub-Processors	Option 2: general written authorization shall apply; prior notice of new Sub-Processors will be given ten (10) days in advance; the method for appointing and objecting to such changes shall be as set forth in Section 8 of the DPA.
Clause 11 – Redress	The optional language shall not apply.
Clause 17 – Governing law	Option 1 shall apply; the Parties agree that the SCCs shall be governed by the laws of the Republic of Ireland.
Clause 18(b) - Jurisdiction	Disputes will be resolved before the courts of the Republic of Ireland.

Annex I.A – List of Parties

	Customer / data exporter	*JFrog / data importer*
Role	Controller	Processor
Relevant activities	Use of the Cloud Services	Provision of the Cloud Services
Name, address, and contact details	As detailed in the Agreement	
Signature and date	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

Categories of Data Subjects and Personal Data	As detailed in Appendix 1 of the DPA
Sensitive Data transferred	Not applicable
Frequency of transfer	Continuous basis for the duration of the Agreement
Nature and purpose of processing	As detailed in Appendix 1 of the DPA
Period for Personal Data retention	As detailed in Appendix 1 of the DPA
For transfers to Sub-Processors	As described above

Annex I.C – Competent Supervisory Authority *(in accordance with Clause 13):*
The data exporter's competent Supervisory Authority will be determined in accordance with the GDPR.

Annex II – Technical and Organizational Measures, as detailed in Appendix 2 to the DPA.

Annex III – List of Subsidiaries and Sub-Processors, as stipulated in Section 8.1 of the DPA.

APPENDIX 4: UK INTERNATIONAL DATA TRANSFER ADDENDUM

1. **Parties.**
   As listed in Annex I.A.

2. **Effective Date.**
   This UK Addendum is effective from the same date as the SCCs.

3. **Background.**
   This UK Addendum is a summarized version of the International Data Transfer Addendum issued by the Information Commissioner Office and is intended to provide the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR ("**Appropriate Safeguards**") for the purposes of Restricted Transfers, when it is entered into as a legally binding contract.

4. **Interpretation.**
   4.1 Where this UK Addendum uses terms that are defined in the SCCs, those terms shall have the same meaning as in the SCCs.
   4.2 If the provisions included in the UK Addendum amend the SCCs in any way which is not permitted under the SCCs or the UK Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the SCCs will take their place.
   4.3 If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
   4.4 Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this UK Addendum has been entered into.

5. **Hierarchy.**
   Where there is any inconsistency or conflict between the UK Addendum and the SCCs, the UK Addendum overrides the SCCs, except where (and in so far as) the inconsistent or conflicting terms of the SCCs provides greater protection for data subjects, in which case those terms will override the UK Addendum.

6. **Incorporation of the Clauses.**
   6.1 This UK Addendum incorporates the SCCs which are deemed to be amended to the extent necessary, so that together they operate for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and to provide Appropriate Safeguards for those

transfers;

6.2 The following amendments to the SCCs are made:

"Clauses"	UK Addendum as it incorporates the SCCs.
"Regulation (EU) 2016/679" and "that Regulation"	Replaced: "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.
"Regulation (EU) 2018/1725"	Removed.
"Union", "EU" and "EU Member State"	Replaced: UK.
Clause 2 - Effect and invariability of the Clauses	Removed: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679"
Clause 6 - Description of the transfer(s)	Replaced: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Appendix A (B) where UK Data Protection Laws apply to the data exporter's processing when making that transfer."
Clause 8.8(i) – Onward Transfers	Replaced: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
Clause 13(a) - Supervision	Not used, the "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner".
Clause 16(e) - Non-compliance with the Clauses and termination	Replaced: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;"
Clause 17 – Governing law	Replaced: "These Clauses are governed by the laws of England and Wales."
Clause 18(b) - Jurisdiction	Replaced: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."
Footnotes	Do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

7. **Amendments to this UK Addendum.**

7.1 The Parties may amend this UK Addendum by agreeing to the changes in writing, provided they maintain the Appropriate Safeguards.

7.2 From time to time, the ICO may issue a revised UK Addendum which will specify the start date from which the changes to the UK Addendum are effective, and whether the Parties need to review it, such revision will be automatically amended from the start date specified.

8. **Executing this UK Addendum.**

8.1 The Parties may enter into this UK Addendum (incorporating the SCCs) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the SCCs.

8.2 By entering into the Agreement and/or DPA, data exporter is deemed to have signed this UK Addendum incorporated herein, as of the Effective Date of the Agreement.