

Controller to Processor Data Processing Addendum

This (Controller to Processor) Data Processing Addendum (“Addendum”) forms a part of the Main Service Agreement (the “Agreement”) entered into between the eBay group company specified in Appendix 2 (“eBay”) and the entity that signed the Agreement (Supplier/Processor), and with eBay, each a “Party” and together, “Parties” on the Effective Date, for the purpose of ensuring that any Personal Data (as defined below) collected or utilized by You is handled in a manner that is secure and otherwise in accordance with terms of the Agreement, this Addendum, and Applicable Data Protection Law. In the event of any conflict between the terms of this Addendum and the terms of the Agreement, prior data processing agreements, addenda, or similar terms between the Parties, the terms of this Addendum shall prevail.

Table of Contents:

1. Definitions
2. Role of the Parties
3. Data Processing Details
4. Sub-Processors
5. Deletion or Return of eBay Data
6. Information Rights and Audits
7. Security Incidents
8. General Terms

Appendix 1 – Basic Nature and Scope of Personal Data Processing

Appendix 2 – eBay Controller Entities

Appendix 3 – Authorized Subprocessor List

Appendix 4 – Additional Regional Privacy Provisions

EU and the UK

United States

Australia

Canada

China

India

Japan

New Zealand

Appendix 5 – Cross-Border Transfer Mechanism

Appendix 6 – China Standard Contractual Clauses for Cross-Border Data Transfers

1. DEFINITIONS

- 1.1. **“Affiliate”** means any entity that directly or indirectly controls, is controlled by or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- 1.2. **“Applicable Data Protection Law”** means applicable law, rule or regulation relating to the privacy, confidentiality, security or protection of Personal Data, as they may be amended from time to time, in the relevant jurisdiction(s) in which data processing occurs. Jurisdictional-specific Applicable Data Protection Laws are outlined in the respective jurisdictions as outlined in this Addendum.
- 1.3. **“Authorized Persons”** means Supplier’s employees, officers, partners, principals, contractors, sub-contractors, Sub-Processors, or other agents who Process eBay Data.
- 1.4. **“Business Purpose”**, or “Processing Purpose” means the use of Data Subject’s Personal Data for eBay’s operational purposes, or other notified purposes, or for the Supplier’s operational purposes, provided that the use of Personal Data shall be reasonably necessary and proportionate to achieve the purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.
- 1.5. **“Controller”** means the natural or legal person that alone or jointly with others determines the purposes and means of the Processing of Personal Data. Controller shall have the same meaning as “Business” under the CCPA.
- 1.6. **“Data Subject”** means the identified or identifiable person to whom Personal Data relates. For purposes of U.S. data processing activities, Data Subject shall have the same meaning as “Consumer” under the CCPA.
- 1.7. **“eBay Data”** includes Personal Data, transactional data, and any reports, analyses, compilations, studies, or other documents that contain or otherwise reflect any of the foregoing. However, for purposes of this addendum, it is limited to Personal Data provided by eBay to Supplier in connection with the provision of the Services, or obtained by Supplier in the course of providing the Services to eBay that pertains to eBay’s employees, customers, users, or other individuals.
- 1.8. **“Personal Data”** or **“Personal Information”** has the meaning given by applicable Laws and shall include information (regardless of the medium in which it is contained), whether alone or in combination with other available information that directly or indirectly identifies an identified or identifiable natural person to whom Personal Data relates. Personal Data shall have the same meaning as Personal Information under applicable Laws.
- 1.9. **“Process”**, **“Processed”** or **“Processing”** means any operation or set of operations that is performed upon eBay Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction.

- 1.10. “**Processor**” means the natural or legal person that Processes eBay Data on behalf of eBay, and which receives from or on behalf of eBay a Data Subject’s Personal Data for a Business or Processing Purpose pursuant to a written contract. For the avoidance of doubt, the term Processor shall also include “Service Provider” and “Contractor” as the terms are defined by Applicable Data Protection Law in the U.S.
- 1.11. “**Regulator**” means any entity which has jurisdiction to enforce the Parties’ compliance with the Applicable Data Protection Law.
- 1.12. “**Restricted Transfer**” means: (i) where the EU GDPR applies, transferring Personal Data collected from a Data Subject located in the EEA either directly or via onward transfer to a country that has not been issued an adequacy determination by the European Commission; (ii) where the UK GDPR applies, transferring, either directly or via onward transfer, Personal Data collected from a Data Subject located in the United Kingdom to or within any other country which is not subject based on adequacy regulations under Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss Federal Act on Data Protection of June 19, 1992 applies, transferring either directly or via onward transfer, Personal Data collected from a Data Subject located in Switzerland to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.
- 1.13. “**Share**”, “**shared**”, or “**sharing**” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, eBay Data by Supplier to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between Supplier and a third party for cross-context behavioral advertising for the benefit of Supplier in which no money is exchanged as set forth under CCPA, as amended by the CPRA.
- 1.14. “**Security Incident**” means a known or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, eBay Data transmitted, stored or otherwise Processed pursuant to the Agreement and this Addendum.
- 1.15. “**Sell**”, “**selling**”, “**sale**”, or “**sold**” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, an eBay Data by Supplier to a third party for monetary or other valuable consideration.
- 1.16. “**Sensitive Data**” or “**Sensitive Information**” means Personal Data or Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. Refer to applicable jurisdictional definition.

- 1.17. **“Sub-Processor”** is the natural or legal person that Processes eBay Data on behalf of the Processor and which receives from or on behalf of the Processor, a Data Subject’s Personal Data.
- 1.18. Terms such as **“Data Protection Officer”**, **“Data Breach”**, **“Sensitive Data”**, and **“Sensitive Personal Information”** shall have the meaning ascribed to them in the Applicable Data Protection Law if the jurisdictional definition differs from what has been ascribed in the Definition section of this Addendum.

2. Role of the Parties

The Parties acknowledge that for the purposes of Applicable Data Protection Law and this Addendum, eBay shall have exclusive authority to determine purposes for and means of Processing eBay Data as the Controller. Supplier is the Processor, or a “service provider” or a “contactor” under California Law, in respect of eBay Data and shall Process eBay Data only on behalf of and for the benefit of eBay in accordance with the terms of the Agreement and this Addendum. All obligations contained in this Addendum shall apply to any Supplier Affiliate who Processes eBay Data under the Agreement. Supplier understands and certifies its compliance with obligations and restrictions imposed on it by Applicable Data Protection Law in its Processing of eBay Data.

3. Data Processing Details

Supplier represents, warrants, agrees that:

- 3.1. **Processing eBay Data.** It shall Process eBay Data only to the extent, and in such a manner, as is necessary for the purposes of fulfilling its obligations under and for the specific Business Purposes set forth in the Agreement and eBay's documented instructions. Any eBay Data will at all times be and remain the sole property of eBay and Supplier will not have or obtain any rights therein, except as may otherwise be agreed to by the parties. For the avoidance of doubt, this Addendum, together with the Agreement and any Order Forms, change orders, or other written directives from eBay, shall constitute all of eBay's documented instructions.
- 3.2. **Processing Sensitive Data.** If Supplier processes any Sensitive Data, as defined under Applicable Data Protection Law, Supplier shall comply with all instructions relating to such Sensitive Data that may be provided by eBay to Supplier or obtained by Supplier on behalf of eBay, including but not limited to, assisting eBay in providing notice and obtaining consent from Data Subject for the Processing of Sensitive Data, and putting into place additional precautions and security safeguards for the Processing of Sensitive Data.
- 3.3. **Compliance with Applicable Law.** Supplier represents and warrants that nothing in the Applicable Data Protection Law prevents it from performing its obligations as described in this Addendum. It shall promptly inform eBay if, in its opinion, a Processing instruction conflicts or infringes an Applicable Data Protection Law. In such case, Supplier shall inform eBay in writing and with specificity of related legal requirement(s), giving details of how eBay instructions conflict or infringe an Applicable Data Protection Law, giving details of eBay Data that it must nevertheless retain before such conflict or infringement is resolved, unless Applicable Data Protection Law prohibits or exempts such information on important grounds of public interest. Supplier shall cooperate in good faith to resolve the conflict or infringement to achieve the goals of such instruction.
- 3.4. **Supplier's Use of eBay Data.** Supplier shall take reasonable actions to assist eBay in ensuring that the Supplier's use of eBay Data is consistent with the obligations under Applicable Data Protection Law and the terms of this Addendum.
- 3.5. **Supplier's Failure to Meet Obligations.** It shall notify eBay immediately if it determines that it can no longer meet its obligations under Applicable Data Protection Law or this Addendum. Upon such notification, eBay shall have the right to take reasonable actions to stop and remediate the Supplier's unauthorized use of eBay Data.
- 3.6. **Disclosure to Third Parties.** Supplier shall not disclose, release, transfer, make available or otherwise communicate any eBay Data to any third party in any circumstances other than in compliance with eBay's documented instructions, or otherwise as permitted by Applicable Data Protection Law, in which case Supplier shall (to the extent permitted by law) notify eBay in writing and liaise with eBay before complying with such disclosure request. Supplier shall immediately notify

eBay in writing upon receipt of an order, demand, or document purporting to request, demand or compel the production of eBay Data to any third party, unless Supplier is prohibited to notify eBay pursuant to Applicable Data Protection Law. Supplier shall not disclose eBay Data to the third party without providing eBay at least forty-eight (48) hours' notice, so that eBay may exercise such rights as it may have under applicable law preventing or limiting such disclosure, unless stipulated otherwise by said applicable law. Notwithstanding the foregoing, Supplier shall exercise reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of eBay Data. Additionally, Supplier shall cooperate with eBay with respect to any action taken pursuant to such order, demand, or other document request, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to eBay Data.

- 3.7. **Confidentiality.** Supplier shall take reasonable steps to ensure that access to eBay Data is limited to Supplier's employees, agents, and subcontractors who (i) have a need to know or otherwise access eBay Data to enable Supplier to perform its obligations under the Agreement and this Australia Addendum, (ii) are bound in writing by confidentiality obligations sufficient to protect the confidentiality of eBay Data in accordance with the terms of the Agreement and this Addendum, and (iii) have completed adequate and appropriate privacy and data security training prior to accessing eBay Data. Supplier shall ensure that all persons granted access to eBay Data shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and Processor shall not permit any person to Process eBay Data who is not under such a duty of confidentiality. Supplier accepts responsibility for any breach of this Addendum caused by the act, error or omission of an Authorized Person.
- 3.8. **Data Subject Requests.** Supplier shall promptly notify eBay of any request it receives from a Data Subject located in the respective jurisdiction(s) for which the Agreement applies concerning the exercise of any rights related to Personal Data provided to Data Subject under Applicable Data Protection Law ("Data Subject Requests"). Supplier shall provide eBay with reasonable assistance to ensure that eBay is able to comply with its obligations concerning any Data Subject Requests, including maintaining the ability to and facilitating eBay's fulfillment of a Data Subject Request (i.e., implementing the technical, organizational and administrative measures necessary to facilitate the access, deletion, modification, or confirmation of Personal Data under Applicable Data Protection Law).
- 3.9. **Regulator Requests.** Supplier shall assist eBay in addressing any communications and abiding by any advice or orders from any Regulator empowered to enforce Applicable Data Protection Law ("Regulator Requests").
- 3.10. **Deidentified Information.** Supplier represents and warrants that to the extent it receives Deidentified Information it shall: (i) take reasonable measures to prevent the reidentification of the Data Subject; (ii) not attempt to reidentify the deidentified information unless required to do so to determine whether the Supplier deidentification processes satisfy the requirements of Applicable Data Protection

Law; and (iii) maintain and use the Deidentified Information in deidentified form. “Deidentified Information” means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject.

3.11. **Notifying a Regulator.** If required by Applicable Data Protection Law, Supplier shall notify the competent Regulator of Supplier’s data processing activities and shall provide eBay with the registration number and all other relevant information and documentation upon request. Supplier shall maintain this registration, and where necessary, renew it during the term of the Addendum. Any changes to Supplier’s status in this respect shall be notified to eBay immediately.

4. Sub-Processors

- 4.1. **Processor's Obligation:** Supplier shall make available to eBay, in Appendix 3 of this Addendum and no later than the Effective Date of the Agreement, an updated list of Sub-Processors with the identities of those Sub-Processors, their services, their country of location, and the legal transfer mechanism required for such transfers.
- 4.2. Supplier's obligations under the Addendum shall apply to any Sub-Processor as set forth in this Addendum. Where Supplier engages a Sub-Processor, equivalent data protection obligations as set out in this Addendum shall be imposed on that Sub-Processor by way of a contract or other legal act under Applicable Data Protection Law. In particular, and where requested by eBay, Sub-Processor shall provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Addendum or Applicable Data Protection Law.
- 4.3. Where Supplier engages a Sub-Processor to process eBay Data, Supplier shall (i) conduct reasonable diligence on such Sub-Processor to attain reasonable assurance that such Sub-Processor complies with its obligations under Applicable Data Protection Law, and (ii) enter into a written contract with the Sub-Processor that imposes obligations that are no less restrictive on the Sub-Processor as is imposed on Supplier under the Agreement and this Addendum. Proof that Supplier has complied with its obligation to provide for sufficient guarantees via a Sub-Processor (commercially sensitive terms may be redacted) shall be provided to eBay promptly upon request.
- 4.4. In the event that eBay reasonably believes a Sub-Processor Processes eBay Data without having provided sufficient guarantees as stipulated above, eBay will inform Supplier without undue delay and the Parties shall cooperate in good faith to resolve the conflict and achieve the goals of such instruction.
- 4.5. Supplier must restrict through technical and organizational measures any Sub-Processor's access to eBay Data to that extent which is strictly necessary to perform its subcontracted processing services to eBay via the Supplier. Additionally, Supplier shall prohibit through technical and organizational measures that the Sub-Processor processes eBay Data for any other purpose. Supplier shall remain fully liable to eBay for the performance of Sub-Processor's obligations where Sub-Processor fails to fulfil its data protection obligations.
- 4.6. Supplier shall also be fully liable for the acts and omissions of its Sub-Processors to the same extent that Supplier would be liable if performing the services of each Sub-Processor directly under the terms of the Agreement and this Addendum.
- 4.7. Supplier may transfer eBay Data to a new Sub-Processor provided that Supplier notifies eBay via email at ebay-privacy-dpa@ebay.com, or via web form at <https://www.ebayinc.com/company/privacy-center/privacy-contact/> that a new Sub-Processor has been acquired. eBay may nevertheless object to Supplier's use of a new Sub-Processor by notifying Supplier in writing within twenty-one (21) business days after receipt of such notice. In the event eBay objects to a new Sub-

Processor, Supplier shall use reasonable efforts to make available to eBay a change in the Services or recommend a commercially reasonable change to eBay within thirty (30) days of eBay's written notice of objection. If Supplier is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, eBay may terminate the Agreement by providing written notice to Supplier. eBay may elect to suspend or terminate the Agreement without penalty and shall receive a prorated refund of any prepaid fees for the period following such termination.

5. Deletion or Return of eBay Data

At the choice of eBay and where applicable, Supplier shall delete or return eBay Data after the end of the term specified in Appendix 1.5.

6. Information Rights and Audits

6.1. Upon eBay's request, Supplier shall provide eBay with reasonable assistance required for eBay to demonstrate and ensure compliance with its obligations under Applicable Data Protection Law, including but not limited to, providing reasonable assistance with any data protection impact assessments or other assessment or measure arising from a Regulator Request.

6.2. Supplier shall, in accordance with Applicable Data Protection Law, make available to eBay such information in Supplier's possession or control as eBay may reasonably request to demonstrate Supplier's compliance with the obligations of Processor under Applicable Data Protection Laws in relation to its Processing of eBay Data. Subject to obligations of confidentiality, Supplier shall make available to eBay its most recent relevant audit report and/or other documentation reasonably required by eBay so that eBay may verify Supplier's compliance with the Agreement and this Addendum.

6.3. Should eBay consider such reports as insufficient to verify Supplier's compliance with its obligations under the Agreement and this Addendum, eBay may request an audit of Supplier's compliance with the Agreement and this EEA/UK Addendum. eBay may not exercise its audit rights more than once in any twelve (12) calendar month period, except (a) if and when required by instruction of a Regulator; or (b) eBay believes a further audit is necessary due to a Security Incident. The audit shall be conducted by an independent third party ("Auditor") reasonably acceptable to Supplier. Prior to the start of an audit, the Parties shall agree to reasonable time, duration, place and manner for the audit.

7. Security Incidents

- 7.1. In the event of an actual or suspected Security Incident impacting eBay Data or any system which houses eBay Data, Supplier shall (i) notify eBay without undue delay but no later than forty-eight (48) hours after Supplier or any Sub-Processor becomes aware of such Security Incident; (ii) provide eBay with sufficient details of the Security Incident to allow eBay to meet any obligations under Applicable Data Protection Law to report or inform U.S. Data Subjects or relevant U.S. regulatory authority of the Security Incident; and (iii) cooperate, and require any Sub-Processor to cooperate with eBay in the investigation, mitigation, and remediation of any such Security Incident.
- 7.2. Supplier's notification of the Security Incident to eBay, to the extent known, shall include: (i) the nature of the Security Incident; (ii) the date and time upon which the Security Incident took place and was discovered; (iii) the number of Data Subjects affected by the Security Incident; (iv) the categories of eBay Data involved; (v) remediation measures – such as encryption, or other technical or organizational measures – that were taken to address the breach, including measures to mitigate the possible adverse effects; and (vi) a description of the likely consequences of the Security Incident.
- 7.3. Supplier shall make no public announcement or communications to any third party regarding such Security Incident without eBay's prior written approval, unless such communication is required by Applicable Data Protection Law.
- 7.4. Upon eBay's request and pursuant to eBay's instructions, Supplier agrees to assist with or perform all remediation efforts required by the contracting eBay entity and Applicable Data Protection Law, or that have been required by regulatory authority in similar circumstances ("Remediation Measures").
- 7.5. To the extent the Security Incident is related to Supplier's acts, omissions or negligence, Supplier's breach of the Agreement, this Addendum, or an Applicable Data Protection Law, Supplier shall be solely responsible for the costs and expenses of all Remediation Measures and all claims arising out of or resulting from such acts, omissions or negligence.

8. General Terms

- 8.1. **Supplier's Failure to Comply.** Supplier's failure to comply with any of the provisions of this Addendum shall be considered a material breach of the Agreement. In such event, eBay may (i) terminate the Agreement effective immediately and Supplier shall return or permanently delete all eBay Data from its computer and storage systems and media, and destroy any and all tangible copies thereof unless eBay Data is required to complete an obligation (i.e., see 8.2.), or (ii) take steps to stop and remediate any unauthorized Processing of eBay Data.
- 8.2. **Expiration or Termination.** Upon expiration or termination of the Agreement for any reason, Supplier's obligations under this Addendum in relation to the Processing of eBay Data shall continue for as long as Supplier has access to eBay Data. Termination or expiration of this Addendum shall not discharge the Supplier (and its Sub-Processor(s)) from obligations meant to survive the termination or expiration of the Agreement.
- 8.3. **Governing Law.** This Addendum shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.
- 8.4. **Severability.** Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either: (i) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.
- 8.5. **Changes to Terms.** Should a change in Applicable Data Protection Law require a variation to this Addendum, the Parties shall agree to discuss and negotiate in good faith the necessary variation to remain compliant with the said Applicable Data Protection Law.

Appendix 1 - Basic Nature and Scope of Personal Data Processing

This Appendix 1 must be completed by the Processor: Please provide as much detail as possible. Enter N/A if not applicable.

This Appendix forms part of the Addendum and describes the basic nature and scope of Personal Data processing carried out by Supplier on behalf of eBay under and/or in connection with the Agreement.

- Purpose(s)** for which Supplier will process Personal Data: (e.g., marketing measures, tracking/targeting services, credit checks, identity checks, maintenance services, etc.)

- _____

- Categories of Personal Data** that may be accessed and/or will be processed pursuant to the Agreement: (e.g., names, address, government issued identification number (SSN), date of birth, IP address, email address, telephone number, device ID, etc.)

- _____

- Special categories of Personal Data** that may be accessed and/or will be processed pursuant to the Agreement: (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)

- _____

- Categories of data subjects** whose Personal Data may be accessed and/or will processed pursuant to the Agreement: (e.g., employees or users, customers, suppliers)

- _____

- Retention Period:** The period for which the personal data will be retained (*if exceeding the term of the Agreement*):

- Term of the Agreement + _____ year(s).

- Which eBay websites, applications, services, products or tools are in **scope of Services** pursuant to the Agreement?

- _____

- Processing locations** Personal Data will be processed by You pursuant to the Agreement:

#	Name of entity (incl legal form)	Role (Supplier – Processor)	Country/Jurisdiction
1.	_____	_____	_____

8. **How will eBay Data be shared with You:** (e.g., manner of transmission/access, department/team(s) handling the data, frequency, etc.)

- _____

9. **Technical and organizational data protection measures** taken by Supplier (e.g., encrypted, on Supplier’s servers, etc.) (For purposes of this section, eBay ISR terms satisfy this question for US-only data transfers. For all other engagements, please answer the question. For engagements where the GDPR applies, Annex II of the SCCs (Appendix 4 Subsection I) shall apply.)

10. Supplier shall take the measures required pursuant to applicable data protection law to ensure the security of processing, including the following measures:

- _____

11. **Specify how Supplier can intake requests from eBay relating to data subjects’ rights:** (Examples: Data subject requests regarding the right to be forgotten can be transferred via an automated API endpoint [provide details]; Data subject requests for access can be submitted via the following online form, e-mail address [provide link or address]):

- _____

12. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

- _____

APPENDIX 2 – eBay Controller Entities

The listed eBay group companies may act as Controller under this Addendum depending on (i) which type of Personal Data is processed and (ii) the region the Data Subjects (users/sellers) are located in:

- Regarding user data: depending on the region in which users as Data Subjects are located, the following eBay group company is responsible for the processing of the users' Personal Data in connection with the use of the marketplace services (except payment services for sellers).
- Regarding payment data: Depending on the region in which sellers as Data Subjects are located and whether payment services are provided there, the following eBay group companies are responsible for the processing of sellers' and buyers' Personal Data in connection with the provision of the payment services to sellers.
- Regarding HR data: The respective eBay group company employing the respective employee (or processing the respective applicant's Personal Data) is responsible for the processing of the employee's/applicant's Personal Data.
- Regarding business contacts data: Each eBay group company maintaining business contacts is responsible for the processing of the Personal Data of the relevant business contacts.

In addition to the eBay group companies listed below, any other eBay group company which (i) is newly founded or acquired or (ii) begins to process Personal Data under or in connection with the Agreement may act as Controller under this Addendum regarding the Personal Data it processes.

#	Name of eBay legal entity incl. legal form	Registered address	Type of Personal Data controlled ¹	Controller for users (eBay platform services) or sellers (eBay payments services) in
1	eBay GmbH	Albert-Einstein-Ring 2-6, 14532 Kleinmachnow, Germany	User data HR data	EU
2	eBay (UK) Limited	1 More London Place, London, SE1 2AF, United Kingdom	User data HR data	UK
3	eBay S.à r.l.	22-24 Boulevard Royal, L-2449 Luxembourg	Payment data	EU

¹ Each Controller listed is also responsible for the processing of its business contacts data where relevant.

4	eBay Commerce UK Ltd	1 More London Place, London SE1 2AF, United Kingdom	Payment data	UK
5	eBay Services S.à r.l.	22-24 Boulevard Royal, 5th Flr., 2449, Luxembourg, Luxembourg	HR data	N/A
6	eBay Customer Support GmbH	Albert-Einstein-Ring 2-6, 14532, Kleinmachnow, Germany	HR data	N/A
7	eBay Group Services GmbH	Albert-Einstein-Ring 2-6, 14532, Kleinmachnow, Germany	HR data	N/A
8	eBay International Management B.V.	Germany Wibaustraat 224, 1097 DN, Amsterdam, Netherlands	HR data	N/A
9	EU Liaison Office BVBA	Kunstlaan 44, 1040 Brussel, Belgium	HR data	N/A
10	eBay Europe Services Limited	The Atrium, Old Navan Road, Blanchardstown, Dublin 15, Ireland	HR data	N/A
11	eBay GmbH, succursale France	21, rue de la Banque, 75002, Paris, France	HR data	N/A
12	eBay France SAS	21, rue de la Banque, 75002, Paris, France	HR data	N/A
13	eBay (UK) Limited, sede secondaria, Milano	Via Roberto Lepetit 8/10, 20124, Milano, Italy	HR data	N/A
14	eBay Spain International, S.L.	Paseo de la Castellana 216 - 9th floor, 28046 Madrid, Spain	HR data	N/A

15	eBay Czech Republic s.r.o.	Nile House, Karolinska 654/2, Prague 8, Karlin, Prague 186 00, Czech Republic	HR data	N/A
----	----------------------------	---	---------	-----

Appendix 3 – Authorized Subprocessor List

- [List authorized Sub-Processors and country of processing with exact company name, legal form, address and scope of sub-processing here, if any.]

Appendix 4 – Additional Regional Privacy Provisions

In addition to the terms set forth in this Addendum, the following Regional Privacy Provisions shall apply to the Supplier’s Processing of eBay Data in the regions outlined below.

EEA, Switzerland, and the United Kingdom

E1. INTERNATIONAL DATA TRANSFERS

- E1.1. To the extent eBay’s use of the Services involves a Restricted Transfer of eBay Data, the terms set forth in Appendix 4 (Cross Border Transfer Mechanisms) shall apply. In the event of any conflict or in-consistency exists between this Addendum and the terms set forth in Appendix 4, in relation to Personal Data collected from individuals while they were located in the EEA, Switzerland or the United Kingdom, the terms in Appendix 4 shall apply.
- E1.2. Insofar as the Agreement involves the transfer of eBay Data from any jurisdiction where GDPR and/or UK GDPR, requires that additional steps, or safeguards, be imposed before eBay Data can be transferred to a second jurisdiction, Supplier agrees to cooperate with eBay to take appropriate steps to comply with GDPR and/or UK GDPR.

United States

U1. Prohibited Use of eBay Data.

Except as specifically permitted by Applicable Data Protection Law, Supplier shall not:

- U1.1 Share, sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, eBay Data to another person or entity for: (a) monetary or other valuable consideration; or (b) cross-contextual behavioral advertising for either monetary or non-monetary benefits.
- U1.2 Retain, use, process, or disclose eBay Data outside of the direct business relationship between eBay and Supplier under the Agreement, or for any business purpose other than for the specific business purpose as outlined in the Agreement or as otherwise permitted by this Addendum or under Applicable Data Protection Law.
- U1.3 Combine eBay Data received from or on behalf of eBay with Personal Data received from or on behalf of any person or collected from Supplier own interaction with a Data Subject or another person or entity.

Australia

A1. Definitions

- A1.1. “**Applicable Data Protection Law**” means any and all Commonwealth, State and Territory laws and regulations of Australia, related to privacy, security, data protection, and/or the Processing of eBay Data, each as amended, replaced or superseded from time to time, including but not limited to (i) the Australia Privacy Act of 1988 (Privacy Act); and (ii) the

Australia Privacy Principles that form part of the Australia Privacy Act of 1988.

- A1.2. Terms such as “**APP Entity**”, “**Sensitive Personal Information**”, “**Sensitive Information**” shall have the meaning ascribed to them in the Applicable Data Protection Law.

A2. International Provisions

- A2.1. To the extent the Supplier’s provision of Services to eBay involves a transfer of eBay Data originating from Australia to another jurisdiction for further processing, Supplier shall take such steps as are reasonable in the circumstances to ensure that transfer does not breach Applicable Data Protection Law.
- A2.2. To the extent the Applicable Data Protection Law requires additional steps or safeguards be imposed before the data can be transferred to another jurisdiction for further processing, Supplier agrees to cooperate with eBay to take appropriate steps to comply with Applicable Data Protection Law.

Canada

C1. Definitions

- C1.1 “**Applicable Data Protection Law**” means any and all federal and provincial and territorial laws and regulations of Canada, related to privacy, security, data protection, and/or the Processing of eBay Data, each as amended, replaced or superseded from time to time, including but not limited to (i) the Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (“PIPEDA”); (ii) Canada’s Anti-Spam Legislation (“CASL”) (ii) the Act respecting the protection of personal information in the private sector of Quebec, CQLR c P-39.1, as amended; (iii) the Personal Information Protection Act of British Columbia, SBC 2003, c 63; and (iv) the Personal Information Protection Act of Alberta, SA 2003, c P-6.5.
- C1.2 “**Processing Purpose**” means the use of Data Subject’s Personal Data for eBay’s operational purposes, or other notified purposes, or for the Supplier’s operational purposes, whether or not by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, managing, storing, adapting, altering, modifying, retrieving, consulting, using, de-identifying, pseudonymizing, anonymizing, disclosing, deleting or destroying the data provided that the use of Personal Data shall be reasonably necessary and proportionate to achieve the purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.
- C1.3 “**Controller**” means organizations that alone or jointly with others determines the purposes and means of the Processing of Personal Data, and

in control of, and accountable for, compliance with privacy law requirements.

- C1.4 **“Sensitive Information”** means Personal Data that include health (i.e., medical records), financial (i.e., income records), sexual practices and preferences, ethnicity, political communication or affiliations, and other data that affect an individual’s reputation (i.e., credit worthiness), or may become sensitive information when combined with other information, that due to its nature or the context of its communication entails a high level of reasonable expectation of privacy and require a higher degree of privacy and technical protections including data subject’s express consent.

C2. Authority to Process eBay Data

- C2.1 Supplier shall not send any commercial electronic messages (“CEMs”), as such term is defined under Canada’s Anti-Spam Legislation (Statutes of Canada 2010, c 23) and its associated regulations (collectively, “CASL”), on behalf of Company, or cause or permit the sending of CEMs on behalf of Company, or otherwise in connection with the EULA or Services Agreement without the prior written consent of Company or as otherwise agreed to or in accordance with the EULA or Services Agreement. If Company provides consent, Service Provider represents, warrants and agrees that it fully complies, and will cause any of its permitted Subprocessors or agents to fully comply, with all applicable consent, notice, unsubscribe and other requirements under CASL.

C3. International Provision

- C3.1 To the extent the Supplier’s provision of Services to eBay involves a transfer of eBay Data originating from the province of Alberta, British Columbia, and Quebec to another province in Canada, or other jurisdictions for further processing, Supplier shall not transfer, or participate in any such transfer without the prior written consent of eBay. To the extent eBay consents to such transfer, Supplier shall take reasonable steps under the circumstances to ensure that transfer does not breach Applicable Data Protection Law, including but not limited to, assist eBay in obtaining additional consent from Data Subject for the transfer, providing necessary information to eBay so that eBay may complete privacy impact assessments.
- C3.2 To the extent the Applicable Data Protection Law requires additional steps or safeguards be imposed before the data can be transferred to another jurisdiction for further processing, Supplier agrees to cooperate with eBay to take appropriate steps to comply with Applicable Data Protection Law.

China

CH1. Definitions

- CH1.1 **“Applicable Data Protection Law”** means any and all laws, regulations, and implementing measures related to privacy, security, data protection, and/or the Processing of eBay Data in China, each as amended, replaced or

superseded from time to time, including but not limited to (i) Geren Xinxi Baohu Fa (the Personal Information Protection Law) promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 01, 2021; (ii) Shuju Anquan Fa (the Data Security Law) promulgated by the Standing Comm. Nat'l People's Cong., Jun. 10, 2021, effective Sep. 01, 2021; (iii) Wangluo Anquan Fa (the Cybersecurity Law) promulgated by the Standing Comm. Nat'l People's Cong., Nov. 07, 2016, effective Jun. 01, 2017.

CH1.2 “**Controller**” means organizations and individuals that alone or jointly with others determines the purposes and means of the Processing of Personal Data, and in control of, and accountable for, compliance with privacy law requirements. For the avoidance of doubt, the term Controller shall also include “Geren Xinxi Chulizhe (Personal Information Handler)” as defined under Applicable Data Protection Law.

CH2. **International Provision**

CH2.1 To the extent the Supplier's provision of Services to eBay involves a transfer of eBay Data originating from China to other jurisdictions for further processing, Supplier shall not transfer, or participate in any such transfer without the prior written consent of eBay. To the extent eBay consents to such transfer, Supplier shall take reasonable steps under the circumstances to ensure that transfer does not breach Applicable Data Protection Law, including but not limited to, providing necessary information to enable eBay to complete any privacy impact assessments as required under Applicable Data Protection Law.

CH2.2 The Parties agree that the Standard Contractual Clauses for Cross-border Data Transfer (“China SCC”) as incorporated in Appendix 5, will apply to any transfer of eBay Data originating from China, either directly or via onward transfer. To the extent there is any conflict between China Addendum and the attached China SCC in relation to the Processing eBay Data originating from China, the terms of the China SCC will prevail.

CH2.3 To the extent the Applicable Data Protection Law requires additional steps or safeguards be imposed before the data can be transferred to another jurisdiction for further processing, Supplier agrees to cooperate with eBay to take appropriate steps to comply with Applicable Data Protection Law.

CH3. **eBay Companies Acting as Controllers**

The listed eBay group companies below may act as Controller for all China-based eBay Data Processing activities under this Addendum. In addition to the eBay group companies listed below, any other eBay group company which (i) is newly founded or acquired or (ii) begins to process personal data under or in connection with the Agreement may act as Controller under this India Addendum regarding the personal data it processes. Please see

Appendix 2 (APPENDIX 2 – CONTROLLER(S)) for details regarding Processing user data, payment data, and HR data.

#	Name of eBay legal entity incl. legal form	Registered address	Type of personal data controlled ²	Controller for users (eBay platform services) or sellers (eBay payments services) in
1	eBay Marketplaces GmbH	Helvetiastrasse 15/17, 3005 Bern, Switzerland	User data HR data	China
2	<insert correct data entity for the jurisd>		Payment data	

India

11. Definitions

- 11.1 **“Applicable Data Protection Law”** means any and all laws, regulations and ordinances, related to privacy, security, data protection, and/or the Processing of eBay Data, each as amended, replaced or superseded from time to time, including but not limited to, the Digital Personal Data Protection Act (No. 22 of 2023).
- 11.2 **“Controller”** means any person alone or jointly with others determines the purposes and means of the Processing of Personal Data. The definition of “Controller” includes “Data Fiduciary” as defined under Applicable Data Protection Law.

12. eBay Companies Acting as Controllers

The listed eBay group companies below may act as Controller for all India-based eBay Data Processing activities under this Addendum. In addition to the eBay group companies listed below, any other eBay group company which (i) is newly founded or acquired or (ii) begins to process personal data under or in connection with the Agreement may act as Controller under this India Addendum regarding the personal data it processes. Please see Appendix 2 (APPENDIX 2 – eBay Controller Entities) for details regarding Processing user data, payment data, and HR data.

#	Name of eBay legal entity incl. legal form	Registered address	Type of personal data controlled ³	Controller for users (eBay platform services) or sellers (eBay payments services) in
1	eBay Singapore Services Private Limited	10 Collyer Quay, #10-01 Ocean Financial Centre, Singapore 049315	User data HR data	India
2			Payment data	

Japan

J1. Definitions

J1.1 “**Applicable Data Protection Law**” means any and all laws, regulations and ordinances, related to privacy, security, data protection, and/or the Processing of eBay Data, each as amended, replaced or superseded from time to time, including but not limited to, the Act on the Protection of Personal Information Act (No. 37 of 2021).

J1.2 “**Business Operator**” (Kojin Joho Toriatsukai Jigyosha) means a business operator using a Personal Information database or the equivalent for business in Japan, as defined under Applicable Data Protection Law.

J1.3 Terms such as “**Sensitive Personal Information**” shall have the meaning ascribed to them in the Applicable Data Protection Law.

J2. eBay Companies Acting as Controllers

The listed eBay group companies below may act as Controller for all Japan-based eBay Data Processing activities under this Addendum. In addition to the eBay group companies listed below, any other eBay group company which (i) is newly founded or acquired or (ii) begins to process personal data under or in connection with the Agreement may act as Controller under this India Addendum regarding the personal data it processes. Please see Appendix 2 (APPENDIX 2 – eBay Controller Entities) for details regarding Processing user data, payment data, and HR data.

#	Name of eBay legal entity incl. legal form	Registered address	Type of personal data controlled ⁴	Controller for users (eBay platform services) or sellers (eBay payments services) in
1	eBay Marketplaces GmbH	Helvetiastrasse 15/17, 3005 Bern, Switzerland	User data HR data	Japan
2	eBay Commerce Japan Pty. Ltd.	Level 18, 1 York Street, Sydney NSW 2000, Japan	Payment data	Japan

New Zealand

NZ1. Definitions

NZ1.1 **“Applicable Data Protection Law”** means any and all New Zealand federal and provincial laws and regulations, related to privacy, security, data protection, and/or the Processing of eBay Data, each as amended, replaced or superseded from time to time, including but not limited to (i) the Privacy Act of 2020, and (ii) the Information Privacy Principles that forms part of the Privacy Act of 2020.

NZ1.2 **“Processing Purpose”** means the use of Data Subject’s Personal Data for eBay’s operational purposes, or other notified purposes, or for the Supplier’s operational purposes, provided that the use of Personal Data shall be reasonably necessary and proportionate to achieve the purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.

NZ1.3 **“Sensitive Personal Information”** means Personal Data revealing Data Subject’s race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural or political beliefs, and membership of an advocacy group, trade union or political party, Personal Data concerning health, genetic, biometric, and financial information, and Personal Data of children or young persons as prescribed under applicable laws.

NZ1.4 Terms such as **“Agency”**, **“Privacy Breach”**, **“Notifiable Privacy Breach”** shall have the meaning ascribed to them in the Applicable Data Protection Law.

NZ2. Supplier Obligations

NZ2.1 Privacy Officer. Supplier shall appoint a Privacy Officer as required under Applicable Data Protection Law, with responsibility for monitoring and ensuring Supplier’s compliance with the Agreement and this Addendum. The Privacy Officer shall cooperate with and provide all reasonable and timely assistance to eBay to enable eBay to (i) fulfill its legal obligations; (ii) formulate a correct response to Data Subject and Regulator requests involving eBay Data; and (c) take suitable further steps in respect to any Security Incident, Data Subject Request, or any other correspondence, inquiry or complaint received from an individual, Regulator, court or other third party in connection with the Processing of eBay Data.

NZ3. eBay Companies Acting as Controllers

The listed eBay group companies below may act as Controller for all New Zealand-based eBay Data Processing activities under this Addendum. In addition to the eBay group companies listed below, any other eBay group company which (i) is newly founded or acquired or (ii) begins to process personal data under or in connection with the Agreement may act as Controller under this India Addendum regarding the personal data it processes. Please see Appendix 2 (APPENDIX 2 – eBay Controller Entities) for details regarding Processing user data, payment data, and HR data.

#	Name of eBay legal entity incl. legal form	Registered address	Type of personal data controlled ⁵	Controller for users (eBay platform services) or sellers (eBay payments services) in
1	eBay Marketplaces GmbH	Helvetiastrasse 15/17, 3005 Bern, Switzerland	User data HR data	New Zealand

Appendix 5 – Cross-Border Transfer Mechanism

1. Definitions

- a. “**EC**” means the European Commission.
- b. “**EEA**” means the European Economic Area.
- c. “**EEA Data**” means eBay Data collected from data subjects when they are located in the EEA.
- d. “**Standard Contractual Clauses**” means (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for transferring personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council (“**EU SCC**”); (ii) where the UK GDPR applies the International Data Transfer Agreement A1.0 issued by the ICO (“**UK IDTA**”), and (iii) where the Swiss FADP applies, the applicable standard data protection clauses issued, approved or recognised by the Swiss Federal Data Protection and Information Commissioner (“**Swiss SCC**”).
- e. “**Swiss Data**” means eBay Data collected from data subjects when they are located in Switzerland.
- f. “**UK Data**” means eBay Data collected from data subjects when they are located in the United Kingdom.

2. Cross Border Data Transfer Mechanisms

- a. **Written Consent.** Supplier shall not transfer, or participate in any transfer of EEA Data, UK Data or Swiss Data to any other jurisdiction without the prior written consent of eBay. To the extent eBay consents to such transfer, Supplier represents and warrants that any onward transfer of EEA Personal Data, UK Personal Data or Swiss Personal Data to a country that is not recognized by the European Commission as providing as adequate level of protection for Personal Data, as described by the EU GDPR, the UK GDPR and the Swiss DPA, complies with applicable legal framework, to ensure the adequate level of security for the data transfer. Upon request, Supplier shall share with eBay copies of its contracts with such Sub-Processors.
- b. **EEA Data.** The parties agree that the Standard Contractual Clauses will apply to any Restricted Transfer of eBay Data from the EEA or Switzerland, either directly or via onward transfer. To the extent there is any conflict between the DPA and the applicable EU SCC in relation to the processing of EEA Personal Data, the terms of the EU SCC will prevail. To the extent applicable, the Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
 - i. Module Two (Controller to Processor) of the Standard Contractual Clauses will apply where eBay is a Controller of eBay Data and Supplier is Processing eBay Data. A copy of Module Two of the EU SCC can be found at:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

- ii. For Module Two, where applicable, the Parties agree that the following terms apply:
- a) in Clause 7, the optional docking clause will not apply;
 - b) certification of deletion of eBay Data that is described in Clause 8.5 of the Standard Contractual Clauses shall be provided by Supplier to eBay only upon eBay's request;
 - c) in Clause 9, Option 2 Use of Subprocessors shall apply and the "time period" for prior notice of Sub-Processor changes will be as set forth in this EEA/ UK Addendum;
 - d) in Clause 11(a), Redress the optional language will not apply;
 - e) in relation to Clause 13(a), see (k) below;
 - f) in Clause 17 (Option 1), the Standard Contractual Clauses will be governed by the law of Germany;
 - g) in Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of Germany;
 - h) Annex I, Part A. LIST OF PARTIES of the Standard Contractual Clauses is deemed completed with information set forth below:
 - a. Data exporter(s): The data exporter(s) is/are the following eBay entity/entities effectuating the transfer(s) of personal data to the data importer:

-
- i. Signature and date: The undersigned has the power of attorney to sign for all data exporters listed in ANNEX IV.
 - ii. Name: Anna Zeiter
 - iii. Address: Chief Privacy Officer
 - iv. Contact person's name, position and contact details: Helvetiastrasse 15/17, 3005 Bern, Switzerland
 - v. Role controller/processor): Controller
- b. Data importer(s):
- i. Name: [SUPPLIER TO COMPLETE]
 - ii. Address: [SUPPLIER TO COMPLETE]
 - iii. Contact person's name, position and contact details: [SUPPLIER TO COMPLETE]
 - iv. Activities relevant to the data transferred under these Clauses: [SUPPLIER TO COMPLETE]
 - v. Signature and date: [SUPPLIER TO COMPLETE]
 - vi. Role (controller/processor): Processor

i) DESCRIPTION OF TRANSFER (Annex 1.B. of the Standard Contractual Clauses)

Categories of data subjects whose personal data is transferred

See Appendix 1 of the DPA.

Categories of personal data transferred

See Appendix 1 of the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Appendix 1 of the DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

One-off transfer Transfer on a continuous basis

Nature of the processing

See Appendix 1 of the DPA.

Purpose(s) of the data transfer and further processing

See Appendix 1 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Appendix 1 of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Appendix 1 of the DPA.

- j) Annex I, Part C of the Standard Contractual Clauses (COMPETENT SUPERVISORY AUTHORITY), depending on the specific service(s) affected as well as the data exporter(s) involved, the competent authority is the following:
 - a. eBay Marketplace Services:
Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow
Tel: +49 33203/356-0
Fax: +49 33203/356-49
Email: Poststelle@LDA.Brandenburg.de
 - b. eBay Payment Services:
Commission Nationale pour la Protection des Données
15, Boulevard du Jazz
L-4370 Belvaux
Tel: +352 2610 60 1
Fax: +352 2610 60 6099
Email: info@cnpd.lu
- k) Annex 2 of the Standard Contractual Clauses

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

[SUPPLIER TO COMPLETE]

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

The data importer uses, as far as possible, strong encryption for the transport and storage of personal data (transport encryption and data-at-rest encryption). Strong encryption requires that

- (a) transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of the third country;
- (b) the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and to be considered robust against cryptanalysis

performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them;

(c) the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved;

(d) the encryption algorithm is flawlessly implemented by properly maintained software.

Further measures of pseudonymisation and encryption of personal data

Description: ...

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Description: ...

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Description: ...

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Description: ...

Measures for user identification and authorization

Description: ...

Measures for the protection of data during transmission

Description: ...

Measures for the protection of data during storage

Description: ...

Measures for ensuring physical security of locations at which personal data are processed

Description: ...

Measures for ensuring events logging

Description: ...

Measures for ensuring system configuration, including default configuration

Description: ...

Measures for internal IT and IT security governance and management

Description: ...

Measures for certification/assurance of processes and products

Description: ...

Measures for ensuring data minimization

Description: ...

Measures for ensuring data quality

Description: ...

Measures for ensuring limited data retention

Description: ...

Measures for ensuring accountability

Description: ...

Measures for allowing data portability and ensuring erasure

Description: ...

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

For transfers to (sub-) processors: The (sub-) processor has taken sufficient technical and organisational measures to be able to provide assistance to the controller.

Description: ...

For transfers from a processor to a sub-processor: The sub-processor has taken sufficient technical and organisational measures to be able to provide assistance to the data exporter.

Description: ...

Not applicable

Further, the Parties agree on the Supplementary Measures as listed in ANNEX IV.

- l) Annex 3 of the Standard Contractual Clauses references Appendix 2.
- c. **Swiss Data.** In accordance with guidance issued by the Swiss Federal Data Protection and Information Commissioner (FDPIC) titled “The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts,” dated 27 August 2021, the parties hereby agree to adopt the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the “EU SCC”) as adapted herein in order to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with Article 6 paragraph 2 letter a of the Federal Act on Data Protection (“FADP”). To the extent there is any conflict between the EEA/ UK Addendum and this Section 2.c, the terms of this section will prevail in relation to Swiss Data. The parties agree that in relation to Restricted Transfer of Swiss Data, Module 2 of the EU SCC apply with the following amendments:
 - i. For purposes of Annex I.C under Clause 13 of Standard Contractual Clauses insofar as the data transfer is governed by the Switzerland Federal Act on Data Protection of 19 June 1992 (SR 235.1; FADP) or the FADP’s revised 25 September 2020 version, the Supervisory Authority shall be Switzerland’s Federal Data Protection and Information Commissioner (FDPIC);
 - ii. The term “member state” must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in Switzerland in accordance with Clause 18(c) of the Standard Contractual Clauses. The Standard Contractual Clauses shall also protect the data of Switzerland legal entities until the entry into force of the 25 September 2020 revised version of the Federal Act on Data Protection (revised FADP). Any references in the Standard Contractual Clauses to “Directive 95/46/EC” or “Regulation (EU) 2016/679” shall be interpreted as references to the Swiss DPA.
- d. **UK Data.** If the processing of eBay Data involves a Restricted Transfer of UK Data, the Parties agree that such transfer(s) will be carried out in accordance with and subject to the International Data Transfer Agreement A1.0 issued by the ICO (“UK IDTA”), which can be found at <https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf>. To the extent there is any conflict between this EEA/ UK Addendum and the UK IDTA in relation to the processing of UK Data, the terms of the UK IDTA will prevail. To the extent applicable, the UK IDTA will be deemed entered into (and incorporated into this EEA/ UK Addendum by this reference) and completed as follows:

i. **Part 1: Tables**

Table 1: Parties and Signatures. See Appendix 5, Section 2.b(ii)(h).

Table 2: Transfer Details

UK country's law that governs the IDTA	<input checked="" type="checkbox"/> England and Wales
Primary place for legal claims to be made	<input checked="" type="checkbox"/> England and Wales
The status of the Exporter	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Exporter is a Controller
The status of the Importer	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor
Whether UK GDPR applies to the Importer	<input checked="" type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data
Linked Agreement	Name of agreement: Main Service Agreement Date of agreement: See Effective Date. Parties to the agreement: See Appendix 5, Section 2.b(ii)(h). Reference (if any): N/A
Term	The Importer may Process the Transferred Data for the following time period: <input checked="" type="checkbox"/> the period which the Importer retains the Transferred Data
Ending the IDTA before the end of the Term	<input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing, or any termination provisions contained in the Agreement or DPA apply.
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2 of the IDTA: <input checked="" type="checkbox"/> Exporter
Can the Importer make further transfers of the Transferred Data?	<input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 of the IDTA (Transferring on the Transferred Data).

Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1 of the IDTA: <input checked="" type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) and other third parties as described in the DPA.
Review Dates	First review date: Terms Effective Date of the DPA The Parties must review the Security Requirements at least once: <input checked="" type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment, to the extent that Importer is made aware of such changes; Importer will conduct a review at the time of contract renewal.

Table 3: Transferred Data. See Appendix 1, which will be updated automatically if the data transferred changes.

Table 4: Security Requirements.

- i. See Appendix 1, subsection 8.
- ii. Part 2: Extra Protection Clauses: N/A.
- iii. Part 3: Commercial Clauses: See the Parties' Main Service Agreement to which this Addendum is attached and incorporated by reference.
- iv. Part 4: Mandatory Clauses: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

APPENDIX 6 – China Standard Contractual Clauses for Cross-Border Data Transfers

个人信息出境标准合同

为了确保境外接收方处理个人信息的活动达到中华人民共和国相关法律法规规定的个人信息保护标准，明确个人信息处理者和境外接收方个人信息保护的权利和义务，经双方协商一致，订立本合同。

个人信息处理者： _____

地址： _____

联系方式： _____

联系人： _____ 职务： _____

境外接收方： _____

地址： _____

联系方式： _____

联系人： _____ 职务： _____

个人信息处理者与境外接收方依据本合同约定开展个人信息出境活动，与此活动相关的商业行为，双方【已】/【约定】于_____年_____

月____日订立（商业合同，如有）。

本合同正文根据《个人信息出境标准合同办法》的要求拟定，在不与本合同正文内容相冲突的前提下，双方如有其他约定可在附录二中详述，附录构成本合同的组成部分。

第一条 定义

在本合同中，除上下文另有规定外：

（一）“个人信息处理者”是指在个人信息处理活动中自主决定处理目的、处理方式的，向中华人民共和国境外提供个人信息的组织、个人。

（二）“境外接收方”是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。

（三）个人信息处理者或者境外接收方单称“一方”，合称“双方”。

（四）“个人信息主体”是指个人信息所识别或者关联的自然人。

（五）“个人信息”是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

（六）“敏感个人信息”是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

（七）“监管机构”是指中华人民共和国省级以上网信部门。

（八）“相关法律法规”是指《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国民法典》《中华人民共和国民事诉讼法》《个人信息出境标准合同办法》等中华人民共和国法律法规。

（九）本合同其他未定义术语的含义与相关法律法规规定的含义一致。

第二条 个人信息处理者的义务

个人信息处理者应当履行下列义务：

（一）按照相关法律法规规定处理个人信息，向境外提供的个人信息仅限于实现处理目的所需的最小范围。

（二）向个人信息主体告知境外接收方的名称或者姓名、联系方式、附录一“个人信息出境说明”中处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

(三) 基于个人同意向境外提供个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

(四) 向个人信息主体告知其与境外接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在 30 日内明确拒绝，则可以依据本合同享有第三方受益人的权利。

(五) 尽合理地努力确保境外接收方采取如下技术和管理措施（综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外接收方的保存期限等可能带来的个人信息安全风险）以履行本合同约定的义务：

（如加密、匿名化、去标识化、访问控制等技术和措施）

(六) 根据境外接收方的要求向境外接收方提供相关法律规定和技术标准的副本。

(七) 答复监管机构关于境外接收方的个人信息处理活动的询问。

(八) 按照相关法律法规对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。重点评估以下内容：

1. 个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性。
2. 出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险。
3. 境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全。
4. 个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等。
5. 按照本合同第四条评估当地个人信息保护政策和法规对合同履行的影响。
6. 其他可能影响个人信息出境安全的事项。保存个人信息保护影响评估报告至少 3 年。

(九) 根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

(十) 对本合同义务的履行承担举证责任。

(十一) 根据相关法律法规要求，向监管机构提供本合同第三条第十一项所述的信息，包括所有合规审计结果。

第三条 境外接收方的义务

境外接收方应当履行下列义务：

(一)按照附录一“个人信息出境说明”所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。

(二)受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。

(三)根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

(四)采取对个人权益影响最小的方式处理个人信息。

(五)个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

(六)按下列方式保障个人信息处理安全：

1. 采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。
2. 确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。

(七)如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问，应当开展下列工作：

1. 及时采取适当补救措施，减轻对个人信息主体造成的不利影响。
2. 立即通知个人信息处理者，并根据相关法律法规要求报告监管机构。通知应当包含下列事项：
 - (1) 发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问的个人信息种类、原因和可能造成的危害。
 - (2) 已采取的补救措施。
 - (3) 个人信息主体可以采取的减轻危害的措施。
 - (4) 负责处理相关情况的负责人或者负责团队的联系方式。
3. 相关法律法规要求通知个人信息主体的，通知的内容包含本项第2目的事项。受个人信息处理者委托处理个

人信息的，由个人信息处理者通知个人信息主体。

4. 记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。

(八)同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息：

1. 确有业务需要。

2. 已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

3. 基于个人同意处理个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

4. 与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律风险。

5. 根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。

(九)受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一“个人信息出境说明”中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。

(十)利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者向个人信息主体提供便捷的拒绝方式。

(十一)承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。

(十二)对开展的个人信息处理活动进行客观记录，保存记录至少 3 年，并按照相关法律法规要求直接或者通过个人信息处理者向监管机构提供相关记录文件。

(十三)同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问、配合监管机构检查、服从监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。

第四条 境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响

(一) 双方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。

(二) 双方声明，在作出本条第一项的保证时，已经结合下列情形进行评估：

1. 出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。

2. 境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素：

- (1) 该国家或者地区现行的个人信息保护法律法规及普遍适用的标准。
- (2) 该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺。
- (3) 该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机关等。

3. 境外接收方安全管理制度和技术手段保障能力。

(三) 境外接收方保证，在根据本条第二项进行评估时，已尽最大努力为个人信息处理者提供了必要的相关信息。

(四) 双方应当记录根据本条第二项进行评估的过程和结果。

(五) 因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。

(六) 境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个人信息要求的，应当立即通知个人信息处理者。

第五条 个人信息主体的权利

双方约定个人信息主体作为本合同第三方受益人享有以下权利：

(一)个人信息主体依据相关法律法规,对其个人信息的处理享有知情权、决定权,有权限制或者拒绝他人对其个人信息进行处理,有权要求查阅、复制、更正、补充、删除其个人信息,有权要求对其个人信息处理规则进行解释说明。

(二)当个人信息主体要求对已经出境的个人信息行使上述权利时,个人信息主体可以请求个人信息处理者采取适当措施实现,或者直接向境外接收方提出请求。个人信息处理者无法实现的,应当通知并要求境外接收方协助实现。

(三)境外接收方应当按照个人信息处理者的通知,或者根据个人信息主体的请求,在合理期限内实现个人信息主体依照相关法律法规所享有的权利。

境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。

(四)境外接收方拒绝个人信息主体的请求的,应当告知个人信息主体其拒绝的原因,以及个人信息主体向相关监管机构提出投诉和寻求司法救济的途径。

(五)个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和境外接收方的一方或者双方主张并要求履行本合同项下与个人信息主体权利相关的下列条款:

1. 第二条,但第二条第五项、第六项、第七项、第十一项除外。
2. 第三条,但第三条第七项第2目和第4目、第九项、第十一项、第十二项、第十三项除外。
3. 第四条,但第四条第五项、第六项除外。
4. 第五条。
5. 第六条。
6. 第八条第二项、第三项。
7. 第九条第五项。

上述约定不影响个人信息主体依据《中华人民共和国个人信息保护法》享有的权益。

第六条 救济

(一)境外接收方应当确定一个联系人,授权其答复有关个人信息处理的询问或者投诉,并应当及时处理个人信息主体的询问或者投诉。境外接收方应当将联系人信息告知个人信息处理者,并以简洁易懂的方式,通过单独通知或者在其网站公告,告知个人信息主体该联系人信息,具体为:

联系人及联系方式(办公电话或电子邮箱)

(二)一方因履行本合同与个人信息主体发生争议的,应当通知另一方,双方应当合作解决争议。

(三)争议未能友好解决,个人信息主体根据第五条行使第三方受益人的权利的,境外接收方接受个人信息主体通过下列形式维护权利:

1. 向监管机构投诉。
2. 向本条第五项约定的法院提起诉讼。

(四)双方同意个人信息主体就本合同争议行使第三方受益人权利，个人信息主体选择适用中华人民共和国相关法律法规的，从其选择。

(五)双方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》向有管辖权的人民法院提起诉讼。

(六)双方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。

第七条 合同解除

(一)境外接收方违反本合同约定的义务，或者境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，个人信息处理者可以暂停向境外接收方提供个人信息，直到违约行为被改正或者合同被解除。

(二)有下列情形之一的，个人信息处理者有权解除本合同，并在必要时通知监管机构：

1. 个人信息处理者根据本条第一项规定暂停向境外接收方提供个人信息的时间超过1个月。
2. 境外接收方遵守本合同将违反其所在国家或者地区的法律规定。
3. 境外接收方严重或者持续违反本合同约定的义务。
4. 根据境外接收方的主管法院或者监管机构作出的终局决定，境外接收方或者个人信息处理者违反了本合同约定的义务。

在本项第1目、第2目、第4目的情况下，境外接收方可以解除本合同。

(三)经双方同意解除本合同的，合同解除不免除其在个人信息处理过程中的个人信息保护义务。

(四)合同解除时，境外接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份）并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

第八条 违约责任

(一)双方应就其违反本合同而给对方造成的损失承担责任。

(二)任何一方因违反本合同而侵害个人信息主体享有的权利，应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应当承担的行政、刑事等法律责任。

(三)双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。

第九条 其他

(一) 如本合同与双方订立的任何其他法律文件发生冲突，本合同的条款优先适用。

(二) 本合同的成立、效力、履行、解释、因本合同引起的双方间的任何争议，适用中华人民共和国相关法律法规。

(三) 发出的通知应当以电子邮件、电报、电传、传真（以航空信件寄送确认副本）或者航空挂号信发往
（具体地址）
或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的__天应当视为收讫；
如以电子邮件、电报、电传或者传真发出，在发出以后的__个工作日应当视为收讫。

(四) 双方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任人而向另一方的追偿，双方应当协商解决；协商不成，任何一方可以采取下列第__种方式加以解决（如选择仲裁，请勾选仲裁机构）：

1. 仲裁。将该争议提交

中国国际经济贸易仲裁委员会

中国海事仲裁委员会

北京仲裁委员会（北京国际仲裁中心）

上海国际仲裁中心

其他《承认及执行外国仲裁裁决公约》成员的仲裁机构_____

按其届时有有效的仲裁规则在（仲裁地点）进行仲裁；

2. 诉讼。依法向中华人民共和国有管辖权的人民法院提起诉讼。

(五) 本合同应当按照相关法律法规的规定进行解释，不得以与相关法律法规规定的权利、义务相抵触的方式解释本合同。

(六) 本合同正本一式_____份，双方各执_____份，其法律效力相同。本合同在（地点）
_____签订

个人信息处理者：_____

_____年_____月_____日

境外接收方：_____

_____年_____月_____日

附录一

个人信息出境说明

根据本合同向境外提供个人信息的详情约定如下：

- （一）处理目的：
- （二）处理方式：
- （三）出境个人信息的规模：
- （四）出境个人信息种类（参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）
- （五）出境敏感个人信息种类（如适用，参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）
- （六）境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）
- （七）传输方式：
- （八）出境后保存期限：
（ 年 月 日至 年 月 日）
- （九）出境后保存地点：
- （十）其他事项（视情况填写）

附录二

双方约定的其他条款（如需要）

