This (Controller to Controller) 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 (Vendor), 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 Vendor is handled in a manner that is secure and otherwise in accordance with terms of the Agreement, the Vendor's obligation as a Controller, 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:

This Independent Controller Data Protection Requirements Addendum and any applicable Appendices, Exhibits, or Annexes (this "DPA" or "Addendum") form part of the *[Master Services Agreement/Services Agreement dated _____]* (the "Agreement") between [name of eBay entity signing the MSA or Services Agreement that owns the contractual relationship with the Data Subject] ("*[name of eBay entity]*" or "eBay" or "eBay Group") and *[name of Vendor as provided in the MSA/Services Agreement]* ("Vendor") (each a "Party" and collectively the "Parties").

1. Scope, Purposes of Processing And Purpose Limitations:

1.1. The transfer of the personal data received by eBay and listed in **Appendix 1** including the categories of data subjects to which they relate has the **following purpose(s)** (i.e. the personal data will processed for the following purpose(s)):

[VENDOR TO COMPLETE]

1.2. The transfer of the personal data received by Vendor and listed in **Appendix 1** including the categories of data subjects to which they relate has the **following purpose(s)** (i.e. the personal data will processed for the following purpose(s)):

[VENDOR TO COMPLETE]

1.3. Vendor shall process personal data received from the other Party exclusively for the purpose(s) described under 1.2. Any further processing of the personal data is not permitted. The transfer of eBay Data by Vendor to third parties for the own purposes of such third parties is not permitted (See Section 4).

1.4. Vendor shall delete the personal data received under this Addendum immediately after the respective purpose(s) described under 1 above has/have been fulfilled (see Section 6). Any further processing of the eBay Data is not permitted except where required under applicable U.S. Data Processing Law or another applicable law (i.e., if a retention obligation applies).

2. Relations and Duties of the Parties:

2.1. Each party shall process personal data received under this Addendum as a separate and independent "Controller" as defined under applicable Data Protection Law. Vendor operates and processes eBay Data as a "Business", "Service Provider" or "Contractor" under California Law where applicable. In no event shall Vendor process personal data under this Addendum as a joint controller to eBay, or in a Controller-to-Processor relationship with eBay where applicable.

2.2. As a separate and independent Controller, Vendor shall be individually and separately responsible and liable for complying with its obligations under applicable Data Protection Law. This includes, but is not limited to the obligation to provide appropriate safeguards for the transfer of personal data to a third country or an international organization where applicable.

2.3. Vendor shall in particular use Security Measures (defined below) (i) to ensure the protection of the rights of any data subject under applicable Data Protection Law, (ii) to ensure the security of personal data from any unauthorized access, (iii) to protect the availability, confidentiality, and integrity of any personal data collected, accessed, used, or transmitted by a party in connection with this Agreement (including but not limited to appropriate data protection and disaster recovery) and (iv) to protect and secure any hosts, networks, applications, and physical premises used while performing under the Agreement. "Security Measures" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of each party's business, the level of sensitivity of the data collected, handled and stored, and the nature of business activities, provided that all such policies, standards, and practices shall, at a minimum, comply with any applicable Data Protection Law and shall consider information security management systems, physical security, physical access control, access control to systems, access control to data, disclosure control, input control, security and privacy enhancing technologies, awareness, training and security checks in relation to the personnel of each party (job control), availability control, segregation control, incident response management/business continuity and audit controls/due diligence.

3. Definitions:

Capitalized terms used but not defined in this Addendum shall have the meaning set forth in the Agreement or the DPA as defined in this section. For the rest, the common definitions of the applicable data protection law apply.

3.1. "**Business Purpose**" means the use of eBay Consumers' Personal Information for eBay's operational purposes, or other notified purposes, or for Vendor' operational purposes, provided that the use of Personal Information shall be reasonably necessary and proportionate to achieve the purpose for which the Personal Information was collected or processed or for another operational purpose that is compatible with the context in which the Personal Information was collected.

3.2. "**eBay Data**" means data or information (regardless of form, e.g., electronic, paper copy, etc.) that Vendor processes independently or on behalf of eBay in providing the agreed-upon services:

3.2.1. "**Confidential Data**": Information that is intended only for a limited audience within eBay or whose release would likely have an adverse financial or reputational effect on eBay, eBay Personnel, or eBay Customers. Examples include, but are not limited to: employee or user personal data (in particular: names, email addresses, physical addresses and any other information that correlates to a person, employee records such as salary, stock and benefits information), software source code, design diagrams, etc.; OR,

3.2.2. "**Restricted Data**": Highly sensitive or regulated information that is intended only for a limited audience within eBay or whose release would likely have a material adverse financial or reputational effect on eBay, eBay Personnel, or eBay Customers. All information in this category is restricted to a limited group with authorized need-to-know access. Examples include, but are not limited to: (i) passwords, challenge/response answers, personal identification numbers (PIN), biometric data, and any other codes that provide access to systems or networks that store, transmit or process eBay Data; (ii) government issued identification numbers (e.g., social security number; driver's license number; state identification number); (iii) financial and payment Information (e.g., bank account numbers, credit card or debit card numbers); (iv) employee or user date of birth; (v) pre-release financial information; (vi) information related to non-public mergers and acquisitions; (vii) medical health records about an individual; and (viii) other information that is specially categorized by applicable laws; OR,

3.2.3. Any personal data processed by Vendor under and/or in connection with the Agreement and/or the DPA received by Vendor as outlined in Appendix 1 of this DPA.

3.3. "**eBay Consumer**" include but are not limited to: end-users or consumers of eBay products or services, prospective users (leads or referrals) of eBay products or services, clients, joint-venture partners, research or study participants (test subjects), or researchers.

3.4. "**Contractor**" is a Supplier/Processor to whom the contracting eBay entity makes available a California resident Data Subject's Personal Information for a Business Purpose pursuant to a written contract under California Law.

3.5. "**Data Protection Law**" means any and all federal, state, or local laws, rules and regulations related to privacy, security, data protection, and/or the Processing of eBay Data, in any relevant jurisdiction, each as amended, replaced or superseded from time to time, including but not limited to the Regulation (EU) 2016/679 ("the GDPR"), and the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.

3.6. "**Personal Data**" mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular eBay Personnel or eBay Customer. Personal Data shall have the same meaning as Personal Data or Personal Information under applicable Data Protection law.

3.7. "**Process**" 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.

3.8. "**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/Processor to a third party for cross-context behavioral advertising, whether or not for monetary or other

valuable consideration, including transactions between Supplier/Processor and a third party for cross-context behavioral advertising for the benefit of Supplier/Processor in which no money is exchanged.

3.9. "**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 Subject Personal Data by the business to a third party for monetary or other valuable consideration.

3.10. "**Service Provider**", or "**Contractor**" is a Business entity within the definition of California law which processes eBay Data on behalf of the contracting eBay entity, and which receives from or on behalf of eBay a California resident personal data for a Business Purpose pursuant to a written contract under California Law.

4. Restrictions and Limitations on Use and Processing of eBay Data:

Vendor represents, warrants and agrees that:

4.1 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 or services as set forth in the MSA, DPA, or otherwise according to eBay's documented instructions.

4.2 Vendor is prohibited from using or processing eBay Data for its own benefits and shall not transmit, share, or otherwise disclose eBay Data with a third party unless expressly permitted to do so by eBay (see 4.4). For avoidance of doubt, this DPA, together with the MSA and any order forms, change orders, or other written directives from eBay, shall constitute all of eBay's documented instructions.

4.3 Vendor shall comply with its obligations and restrictions imposed on it by applicable Data Protection Law in its role as a Business, Service Provider, Contractor under California law, or otherwise as a Controller under another applicable Data Protection Law.

4.4 Vendor shall not disclose personal data to any third party in any circumstances other than to fulfill its obligations under applicable Data Protection Law, or as expressly permitted to do so by the terms of the MSA or this DPA. Furthermore, unless the disclosure is otherwise required by an applicable law, Vendor shall only disclose eBay Data to a third party with a prior written notice to eBay providing eBay the right to exercise such right to limit such a disclosure on a case-by-case basis where permissible under an applicable Data Protection Law. Notwithstanding the foregoing, Vendor shall exercise reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of eBay Data at all times.

4.5 Vendor shall cooperate with eBay with respect to any action taken pursuant to an order, demand, or other document request, including to obtain an appropriate protective order or other reliable assurance that confidential treatment shall be accorded to eBay Data. Vendor shall nevertheless immediately notify eBay in writing upon receipt of such order, demand, or document purporting to request, demand, or compel the production of eBay Data to any third party, including a regulatory authority, unless Vendor is prohibited from notifying eBay pursuant to applicable Data Protection Law or another applicable law.

4.6 If it processes any sensitive personal information, Vendor shall comply with all eBay's documented instructions relating to such sensitive personal information as defined by applicable Data Protection Law.

4.7 Vendor shall inform eBay if, in its opinion, an eBay documented instruction infringes an applicable Data Protection Law, and it shall take reasonable actions to assist eBay in ensuring that Vendor' use of eBay Data is consistent with its obligations under said Data Protection Law.

4.8 Vendor shall notify eBay immediately if it determines that it can no longer meet its obligations under applicable Data Protection Law, the terms of the MSA, or this DPA. Upon such notification, eBay shall have the right to take reasonable actions to stop and remediate Vendor' unauthorized use of eBay Data.

4.9 Except as specifically permitted by applicable Data Protection Law, Vendor shall not under CCPA:

i. 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-context behavioral advertising for the benefit of a business in which no money is exchanged.

ii. Retain, use, or disclose eBay Data outside of the direct business relationship between eBay and Vendor under the MSA, or for any purpose other than for the specific purpose as outlined in the MSA or as otherwise permitted by this DPA.

iii. Combine eBay Data received from or on behalf of eBay with Personal Information received from or on behalf of any person or collected from Vendor own interaction with a Data Subject.

iv. Use, retain, store, disclose, or other Process eBay Data Sensitive Personal Information for any purpose except for those as set forth in the DPA or the Agreement.

v. Process eBay Data Sensitive Personal Information received for any purpose except for purposes authorized by eBay instructions.

5. Use of De-Identified eBay Data:

Vendor represents and warrants that to the extent it receives De-Identified eBay Data it shall: (i) take reasonable measures to prevent the reidentification of the eBay Consumer; (ii) not attempt to reidentify the De-Identified information unless required to do so to determine whether Vendor' deidentification processes satisfy the requirements of applicable Data Protection Law; and (iii) maintain and use the De-Identified eBay Data in deidentified form.

6. Deletion of eBay Data:

At the choice of eBay and upon request, or at the termination of the terms of the Agreement, Vendor shall delete or return all eBay Data relating to the processing as set forth under the MSA and the DPA, and delete existing copies unless Vendor is prohibited to do so by an applicable Data Processing Law requiring retainment of the eBay Data for a specific duration.

7. Effect on Existing Agreements:

Except as specifically modified by the terms of this Addendum, the terms, rights and responsibilities under the MSA shall remain in full force and effect at all times. Notwithstanding the foregoing, violation of the terms of this Addendum shall not be subject to the limitation of liability provision(s) of the MSA.

8. Conflict:

If and to the extent language in this Addendum or any of its Exhibits or Annexes conflicts with the terms of the MSA, this Addendum or any of its Exhibits or Annexes shall control.

9. General:

Each party represents and warrants that this Addendum has been duly authorized, executed and delivered by it and constitutes a valid and legally binding agreement with respect to the subject matter contained herein. This DPA may be signed in any number of counterparts, each of which shall be an original, with the same effect as if the signatures thereto and hereto were upon the same instrument. Signed counterparts may be transmitted by email as a scanned document with the same effect as if they had been manually signed and delivered.

Agreed and accepted for and on behalf of:

[Name of eBay entity]	Vendor: _____
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix 1 to the eBay Independent Controller Data Processing Addendum

1. Personal data received by eBay

eBay will receive the following categories of personal data from Vendor relating to the categories of data subjects mentioned below:

a) Categories of data subjects
- _____

b) Categories of personal data
- _____

2. Personal data received by Vendor

Vendor will receive the following categories of personal data from eBay relating to the categories of data subjects mentioned below:

[VENDOR TO COMPLETE]

c) Categories of data subjects
- _____ _____

d) Categories of personal data
- _____ _____

e) Vendor will process personal data in the following geographical locations:
- _____

f) Will Vendor process personal data relating to individuals located in the EU/EEA/Switzerland/UK?
- _____

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 controlled1	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 datan	UK
3	eBay S.à r.l.	22-24 Boulevard Royal, L-2449 Luxembourg	Payment data	EU
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

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

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 – Cross-Border Transfer Mechanisms

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. **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 One (Controller to Controller) of the Standard Contractual Clauses will apply where eBay is a Controller of eBay Data and Vendor is also a Controller of eBay Data. A copy of Module One 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 One, where applicable, the Parties agree that the following terms apply:

a) in Clause 7, the optional docking clause will not apply;
b) for Clause 8.1, the data importer declaration of "Description of Transfer" in Section j shall apply;
c) for Clause 8.5(b), the "Technical and Organizational Measures Including Technical And Organizational Measures To Ensure The Security Of The Data" in Section k shall apply;
d) in Clause 11(a), "Redress" the optional language shall not apply;
e) in relation to Clause 13(a), see (m) below;
f) in Clause 17, 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 entitiy/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: [VENDOR TO COMPLETE]
ii. Address: [VENDOR TO COMPLETE]
iii. Contact person's name, position and contact details: [VENDOR TO COMPLETE]
iv. Activities relevant to the data transferred under these Clauses: [VENDOR TO COMPLETE]
v. Signature and date: [VENDOR TO COMPLETE]
vi. Role (controller/processor): CONTROLLER

i) **DESCRIPTION OF TRANSFER** [VENDOR TO COMPLETE]

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

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.

…

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

…

Purpose(s) of the data transfer and further processing

…

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

…

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

…

j) **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA** [VENDOR 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 Section l (ANNEX V of the SCC).

k) ADDITIONAL SAFEGUARDS TO THE STANDARD CONTRACTUAL CLAUSES ("SUPPLEMENTARY MEASURES")

(A) Following the Parties' joint effort to assess the risks for data subjects affected by the respective data processing activities of the Parties, the Parties decided to supplement the Clauses as set out in the following.

(B) Nothing in these Supplementary Measures shall limit or exclude any rights of data subjects granted in the Clauses or applicable data protection laws, in particular the General Data Protection Regulation (GDPR) or any obligations of either Party arising from or in connection with the Clauses.

1. General requirements

The Parties undertake to adapt or replace these Supplementary Measures as soon as the European Commission makes available any mechanism that provides adequate safeguards for the transfer of personal data to the data importer. The same applies to adjustments following recommendations of the European Commission and/or the competent data protection authorities.

2. Processing restrictions

Data importer will not disclose personal data except (1) as data exporter directs or (2) where the transfer is in accordance with the provisions of the Clauses and these Supplementary Measures.

3. Data access for public authorities

Notwithstanding Clause 15 of the Clauses, data importer warrants the following:

3.1 Data importer agrees to adopt

(a) adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of covert or official requests from public authorities to access the data;

(b) strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle.

Data importer will regularly review these internal policies to assess their suitability and identify and implement additional or alternative solutions when necessary.

3.2 If data importer is contacted with a legally binding request from a public authority, including judicial authorities, or becomes aware of any direct access by a public authority to the personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination, data importer will attempt to redirect the public authority to request that personal data directly from data exporter instead.

3.3 Data importer will only provide personal data if, and to the extent that, it is necessary and proportionate to comply with a legally binding request. Data importer will not provide any public authority:

(a) blanket, or unfettered access to personal data;

(b) encryption keys used to secure personal data or the ability to break such encryption; or

(c) access to personal data if data importer is aware that the personal data is to be used for purposes other than those stated in the legally binding request.

3.4 In support of the above, data importer may provide data exporter's basic contact information to the public authority. The data importer will notify data exporter in this case, unless data importer is legally restricted to do so.

3.5 The data importer agrees to document the steps taken pursuant to Sections 3.1-3.4 for the duration of the contract and make it available to the competent supervisory authority upon request.

4. Encryption

The data importer warrants that that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key.

l) Annex I, Part C of the Standard Contractual Clauses

COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13
Depending on the specific service(s) affected by the Clauses as well as the data exporter(s) involved the competent authority is the following:

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

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

m) Annex 3 of the Standard Contractual Clauses references Appendix 2 – eBay Controller Entities.

b. **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);

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.

c. **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.a(ii)(h).

Table 2: Transfer Details

UK country's law that governs the IDTA	☒ England and Wales
Primary place for legal claims to be made	☒ England and Wales
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller
The status of the Importer	In relation to the Processing of the Transferred Data: ☒ Importer is the Exporter's Processor or Sub-Processor
Whether UK GDPR applies to the Importer	☒ 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.a(ii)(h). Reference (if any): N/A
Term	The Importer may Process the Transferred Data for the following time period: ☒ the period which the Importer retains the Transferred Data
Ending the IDTA before the end of the Term	☒ 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: ☒ Exporter
Can the Importer make further transfers of the Transferred Data?	☒ 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: ☒ 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:

	☒ 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 5, Sections j and k.

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 4 – 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。

1.1 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。

1.2 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、访问控制等技术和管理措施）

（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。

1.3 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责任。

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。

1.4 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构等。

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。

1.5 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。

1.6 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。

1.7 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的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。

1.8 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。

1.9 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而向另一方的追偿，双方应当协商解决；协商解决不成的，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

2. 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）