[Translation]

Data Processing Addendum

The provisions of this Data Processing Addendum (this “Addendum”; the clauses in this Addendum are hereinafter referred to as the “Clauses” and the agreement pertaining to these Clauses is hereinafter referred to as this “Agreement”) apply to the Processing of Personal Data subject to the Applicable Data Protection Laws (as defined in Clause 1(1)) that SoftBank Corp. (“SoftBank”) conducts based on instructions or choice of the customer in the operations or services provided by SoftBank and designated in the relevant terms of use or agreement (the “Services”). In these Clauses, the customer is in the position of a “Controller,” and SoftBank is in the position of a “Processor,” under the Applicable Data Protection Laws.

These Clauses form part of the terms of use or the agreement for the Services (the “Terms of Use”). In addition, the obligations and responsibilities arising from these Clauses that SoftBank bears in respect of the customer in relation to compliance with the Applicable Data Protection Laws are limited to those set forth in these Clauses.

These Clauses shall be understood and interpreted in the light of the provisions of the Applicable Data Protection Laws and shall not be interpreted in a way that runs counter to the rights and obligations provided for in the Applicable Data Protection Laws or in a way that prejudices the fundamental rights and freedoms of the Data Subjects.

SECTION I

Clause 1 Definitions

The following terms as used in these Clauses shall have the meanings set forth below; provided, however, that the definitions in the Applicable Data Protection Laws shall apply to terms that are not defined in these Clauses.

(1) “Applicable Data Protection Laws” collectively means the data protection and privacy laws of any relevant jurisdictions which are applicable to Processing of Personal Data set out in Annex I, including, where applicable, the regulations, ordinances, decrees, circulars, decisions, guidance, standards, and codes of practice issued by relevant Supervisory Authorities or other competent authorities of relevant jurisdictions.

(2) “Controller” means the natural or legal person, public authority, agency or other body which, independently or jointly with others, determines the purposes and means of Processing of Personal Data, and similar terms defined under the Applicable Data Protection Laws.

(3) “Data Subject” means an identified or identifiable natural person (i.e., one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), and similar terms as defined in the Applicable Data Protection Laws.

(4) “Personal Data” means any information relating to a Data Subject, and similar terms defined under the Applicable Data Protection Laws.

(5) “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed, and similar terms defined under or determined in accordance with the Applicable Data Protection Laws.

(6) “Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and similar terms defined under the Applicable Data Protection Laws.

(7) "Processor" means the natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of Controller, and similar terms defined under the Applicable Data Protection Laws.

(8) "Supervisory Authority" means any public authority responsible for monitoring, inspecting, enforcing, or judging the application of and compliance with the Applicable Data Protection Laws.

(9) "End User" means an individual who utilizes information and communication services (if any) provided by the customer.

Clause 2 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements that are existing at the time when these Clauses are agreed or that are agreed thereafter, these Clauses shall prevail.

SECTION II – OBLIGATIONS OF SOFTBANK AND THE CUSTOMER

Clause 3 Description of Processing

The details of the Processing operations, in particular the categories of Personal Data and the purposes of Processing for which the Personal Data is Processed on behalf of the customer, are specified in Annex I, and SoftBank shall Process Personal Data for such Processing purposes only, unless SoftBank receives additional instructions from the customer.

Clause 4 Obligations and rights of SoftBank and the Customer

4.1. Obligations and rights of the Customer

(a) The Customer is responsible for assessing the lawfulness of the Processing, and for safeguarding the rights of the Data Subjects;

(b) The Customer reserves the right to issue instructions to SoftBank with regard to the matters concerning the Processing of Personal Data. Individual instructions and amendments thereof must always be documented.

(c) Where required by the Applicable Data Protection Laws, the Customer shall conduct a personal information protection impact assessment for the entrustment of Processing beforehand and keep a record of the Processing.

4.2. Instructions

(a) SoftBank shall Process Personal Data only on documented instructions from the customer (which shall be deemed to include instructions provided in Annex IV California Consumer Privacy Act (CCPA) instructions as applicable), unless required to do so by a relevant law or regulation to which SoftBank is subject. In this case, SoftBank shall inform the customer of that legal requirement before Processing, unless the law or regulation prohibits such notice on important grounds of public interest. Subsequent instructions may also be given by the customer throughout the duration of the Processing of Personal Data.

(b) SoftBank shall immediately inform the customer if, in SoftBank's opinion, instructions given by the customer infringe the Applicable Data Protection Laws.

4.3 Security of Processing

(a) SoftBank shall implement appropriate technical and organisational measures to ensure an appropriate level of security to protect Personal Data against unauthorised access and loss, destruction, damage, alteration or disclosure, or against other unlawful processing.

(b) For this purpose, SoftBank shall implement at least the technical and organisational measures specified in Annex II to ensure the security of the Personal Data and any subsequent written amendments ensuring its appropriateness with regard to risks that may evolve over time which are agreed upon by the customer and SoftBank. In assessing the appropriate level of security, SoftBank and the customer shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks of varying likelihood and severity for the rights and freedoms of the Data Subjects concerned.

(c) SoftBank shall grant access to the Personal Data undergoing Processing to its officers, employees and any other persons only to the extent strictly necessary for implementing, managing and monitoring of this Agreement. SoftBank shall ensure that officers, employees and any other persons authorised to Process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.4 Documentation and Compliance

(a) At least once every 12 months, SoftBank shall provide the customer with information (including a copy of a certificate certified by a third party) necessary to demonstrate compliance with the obligations that are provided for in these Clauses and stem directly from the Applicable Data Protection Laws.

(b) Only if there is an indication of non-compliance with these Clauses by SoftBank and the provision of information set forth above (see Clause 4.4 (a)) is insufficient to demonstrate compliance with these Clauses, the customer may, after notifying SoftBank in writing at least 30 days in advance, conduct an on-site audit at the SoftBank by the customer or through a third party auditor (who must not be a competitor of SoftBank and with prior authorisation of SoftBank) up to once a year during the ordinary business hours of SoftBank to the extent such audit does not hinder daily operations of SoftBank or infringe its obligations under a contract with another contractor. The customer and SoftBank shall agree on the scope, timing and duration of audit and confidentiality, etc. before the commencement of an on-site audit. The customer shall bear audit costs, unless separately agreed.

(c) SoftBank and any person acting under the authority of the customer or SoftBank, who has access to Personal Data, shall not Process those data except on instructions from the customer, unless required to do so by a relevant law or regulation.

4.5 Use of Subprocessors

(a) The customer shall give general authorisation for the SoftBank's engagement of subprocessors listed in Annex III.

(i) SoftBank shall give the customer though appropriate ways including emails in advance a specific notice of any intended changes of the subprocessors through the addition or replacement of subprocessors, thereby giving the customer sufficient time to be able to object to such changes prior to the engagement of the concerned subprocessors. If requested by the customer, SoftBank shall provide the customer with the information necessary to enable the customer to exercise the right to object.

(ii) If the customer does not object in writing with grounds within 30 days of the abovementioned notice pertaining to the change of the subprocessors, the customer shall be considered to have given authorisation to such change, and SoftBank thereby may use and engage such subprocessors for carrying out specified Processing operations.

(iii) Even though the customer lawfully objects during the period set forth above, if SoftBank does not make a reasonable response, the customer may cancel the agreement for the Services to the extent affected, without paying additional money, such as penalties, by notifying SoftBank in writing within 30 days from the date of objection.

(iv) If the customer objects during the period set forth above, SoftBank may cancel the agreement for the Services to the extent affected, without paying additional money, such as damages.

(b) Where SoftBank engages a subprocessor for carrying out specific Processing activities (on behalf of the customer), such engagement shall be by way of a contract which imposes on the subprocessor, in substance, the same data protection obligations as the ones imposed on

SoftBank in accordance with these Clauses. SoftBank shall ensure that the subprocessor complies with the obligations to which SoftBank is subject in accordance with these Clauses and the Applicable Data Protection Laws and shall remain fully responsible to the customer for the performance of the subprocessor's obligations.

4.6 International Transfers

Any transfer of data to a third country by SoftBank shall be done in accordance with the Applicable Data Protection Laws.

Clause 5 Assistance to the Controller

(a) SoftBank shall promptly notify the customer of any request it has received from the Data Subject pursuant to the Applicable Data Protection Laws.

(b) SoftBank shall assist the customer in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights laid down in the Applicable Data Protection Laws, taking into account the nature of the Processing. In fulfilling its obligations in accordance with the preceding item and this item, SoftBank shall comply with the customer's instructions.

(c) In addition to SoftBank's obligation to assist the customer pursuant to the preceding items, SoftBank shall furthermore assist the customer in ensuring compliance with the following obligations, taking into account the nature of the data Processing and the information available to SoftBank:

(i) the obligation to carry out an assessment of the impact of the envisaged Processing activities on the protection of Personal Data (a "Data Protection Impact Assessment") where a type of Processing of Personal Data is likely to result in a high risk to the rights and freedoms of natural persons or where required under the Applicable Data Protection Laws;

(ii) the obligation to consult the competent Supervisory Authorities prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the customer to mitigate the risk; and

(iii) the obligations to take the appropriate technical and organisational measures in accordance with the Applicable Data Protection Laws to ensure a level of security appropriate to risks.

(d) SoftBank and the customer shall set out in Annex II the appropriate technical and organisational measures by which SoftBank is required to assist the customer in the application of this Clause as well as the scope and the extent of such assistance.

Clause 6 Notification of Personal Data Breach

(a) In the event of a Personal Data Breach concerning data Processed by SoftBank, SoftBank shall cooperate with and assist the customer for the customer to comply with its obligations to notify a Supervisory Authority or Data Subject of the Personal Data Breach in accordance with the Applicable Data Protection Laws, where applicable, taking into account the nature of the Processing and the information available to SoftBank.

(b) In the event of a Personal Data Breach concerning data Processed by SoftBank, SoftBank shall notify the customer without undue delay after SoftBank having become aware of the Personal Data Breach. Such notification shall contain, at least:

(i) a description of the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned);

(ii) the details of a contact point where more information concerning the Personal Data Breach can be obtained; and

(iii) its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects.

(iv) by the customer's request, other compulsory content that the customer must notify to the Supervisory Authorities under the Applicable Data Protection Laws.

Where, and insofar as, it is not possible to provide all the information above at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

SECTION III FINAL PROVISIONS

Clause 7 Non-Compliance with these Clauses and Termination

(a) Without prejudice to any provisions of the Applicable Data Protection Laws, in the event that SoftBank is in breach of its obligations under these Clauses, the customer may instruct SoftBank to suspend the Processing of Personal Data until SoftBank complies with these Clauses or this Agreement is terminated. SoftBank shall without undue delay inform the customer in case SoftBank is unable to comply with these Clauses, for whatever reason.

(b) SoftBank shall be entitled to terminate this Agreement and the Terms of Use where, after having informed the customer that the customer's instructions infringe applicable legal requirements in accordance with Clause 4.2(b), the customer insists on compliance with the instructions.

(c) Following non-effectiveness, invalidity, revocation, or termination of this Agreement, SoftBank shall delete all Personal Data (including existing copies; the same applies hereinafter in this item) unless a relevant law or regulation requires storage of the Personal Data. The customer shall back up and download or otherwise transfer the Personal Data at its responsibility before this Agreement does not take effect, or is void, revoked, or terminated; provided, however, that SoftBank shall return the Personal Data to the customer if the customer has notified SoftBank in writing to the effect that the customer desires the Personal Data to be returned no later than 30 days of non-effectiveness, invalidity, revocation, or termination of this Agreement and if such return is possible physically. If the customer terminates this Agreement for any reason attributable to the customer, Personal Data shall not be returned to the customer. Until the data is deleted or returned, SoftBank shall continue to ensure compliance with these Clauses.

Clause 8 Liability

(a) SoftBank agrees and warrants that if SoftBank is held liable for a breach of the terms and conditions of this Agreement, SoftBank will, to the extent to which it is liable, indemnify the customer for any cost, charge, damages, expenses or loss the customer has incurred, except for (administrative) fines imposed on the customer.

(b) SoftBank shall not be liable for any damages or (administrative) fines to the extent such damages or (administrative) fines are caused, directly or indirectly, by any act or omission of the customer.

(c) Customer shall indemnify and hold SoftBank harmless against all claims, actions, third party claims, losses, damages and expenses incurred by SoftBank and arising directly or indirectly out of or in connection with a breach of this DPA and/or the Data Protection Laws by the customer.

SECTION IV ADDITIONAL CLAUSES

Clause 9 Force Majeure

SoftBank shall not be liable to compensate the customer if SoftBank is unable to perform or is delayed in the performance of its obligations provided for in these Clauses due to a natural disaster, strike, public disturbance, war, epidemic or other force majeure.

Clause 10 Users of the Services

If any Controller other than the customer (including a parent company, subsidiary or affiliate, etc. of the customer) uses the Services, the customer shall be the agent for any such Controller other than the customer in respect of the rights and obligations under these Clauses. If any Controller other than the customer has the right to make direct claims to SoftBank, the customer shall exercise such right. The customer shall obtain necessary consents from any Controller other than the customer. SoftBank shall be considered to have performed its obligation to notify of and provide information to any Controller other than the customer if SoftBank notifies of or provides the information to the customer.

Clause 11 Governing law and Jurisdiction

This Agreement is governed by the laws of Japan. Any disputes arising from or in connection with this Agreement shall be brought exclusively before the competent court of the Tokyo District Court as the first instance court.

Annex I: Description of the Processing

Subject matter of the Processing:

The subject matter of the Processing (i.e. the main object of the Processing) is set forth in the Terms of Use.

Categories of Data Subjects whose Personal Data is Processed:

Unless otherwise agreed in the Terms of Use, the categories of Data Subjects whose Personal Data is Processed include the following categories of Data Subjects, depending on the Controller's use of the Services.

- Employees of the Controller
- Employees of business partners of the Controller
- Employees of customers of the Controller
- End consumers/users of the Controller
- End consumers/users of the customers/business partners of the Controller

Categories of Personal Data Processed:

Unless otherwise agreed in the Terms of Use, the Personal Data Processed include the following categories of Personal Data, depending on the Controller's use of the Services.

- Name and surname
- Personal address
- Professional address
- Personal telephone number
- Professional telephone number
- E-mail address
- Software/system user accounts
- Network information (IP address, network name)
- E-mails, communications and files
- Professional information and documents (e.g., work files)
- Financial information and documents (e.g., accounts, salaries, financial statements)
- Personal information and documentation (e.g., pictures, personal documents)

Sensitive data Processed and applied restrictions or safeguards (that fully take into consideration the nature of the data and the risks involved):

Unless otherwise agreed in the Terms of Use, the Controller may allow SoftBank to Process sensitive data, depending on the Controller's use of the Services, and the restrictions or safeguards described in Annex II shall apply to the Processing of sensitive data.

- Web browsing history
- Content of mails, emails and text messages
- Account credentials including financial account information
- Financial asset/transaction information

- Personal identification numbers/documents
- Biometric information
- Medical/health information

Nature, Purposes and Duration of the Processing:

Nature of the Processing	Purposes of the Processing	Duration of the Processing
Unless otherwise specified in the Terms of Use, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, depending on the Controller’s use of the Services.	Unless otherwise agreed in the Terms of Use, provision and improvement of the Services pursuant to the Terms of Use.	Unless otherwise agreed in the Terms of Use, during the valid term of the Terms of Use.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data

The specific details of the appropriate technical and organisational measures to protect Personal Data that are taken by SoftBank are set out in the following; provided, however, that if there are any additions stipulated in the Service specifications or descriptions, etc., such additions shall apply in priority to these measures.

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding Personal Data. These measures include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries
- Control the import and export of supplementary storage device (mobile hard drive disk (HDD), USB memory, etc.)

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems and PC/mobile device of users. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (including special characters, minimum length, change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from management
- Limit access authority by ID authentication
- Detection and response to illegal attempts to acquire Personal Data by analyzing the IP addresses that accessed to IT systems
- Automatic disconnection after a period of inactivity

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights. These measures include:

- Differentiated access rights
- Access rights defined according to duties
- Immediate modification or revocation of access rights upon changes of duties
- Recording of access rights granting, modification, and revocation details, and retention of these records
- Issuance of individual accounts per user and prohibition of account sharing, provided, however, that in unavoidable cases, such as when multiple accounts cannot be created due to system specifications, accounts may be shared, under the condition that appropriate account controls are in place under Applicable Data Protection Laws
- Adoption of additional authentication methods
- Restriction of IT system access after a specified number of failed authentication attempts
- Automated log of user access via IT systems and its storage and measures to securely protect these logs

- Monthly review of automated logs of user access
- Verification of the reason for Personal Data downloads identified during the monthly review, in accordance with internal privacy regulation or related policies
- Safety measures to securely manage printed and copied materials containing Personal Data (including specifying the purpose of the data when printed and minimizing the printed items based on that purpose)

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data
- Encryption using a safe encryption algorithm during the transmission of authentication information (such as passwords and biometric data)

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom is maintained. The level of details of the above measures is specific to each environment. These measures include:

- Logging user activities on IT systems

6. Job control

Measures should be put in place to ensure that data is Processed strictly in compliance with the customer's instructions. These measures include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss. These measures include:

- Backup procedures
- Emergency response manual for disasters and incidents
- Uninterruptible power supply (UPS)
- Enterprise Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems with automatic daily update function
- Response measure against any malware discovered
- Prompt implement updates in accordance with issued alerts related to malware or security update notices from anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be Processed separately. These measures include:

- Restriction of access to data stored for different purposes according to staff duties
- Segregation of business IT systems (i.e. logical separation and where possible separate servers)
- Segregation of IT testing and production environments

9. Encryption control

Measures should be put in place to store specific data. These measures include:

- One-way encryption when storing all passwords
- Encryption when storing resident registration number; passport number, driver's license number, alien registration number (collectively "Unique Identification Data") of Data Subjects who are not End Users in the internet network segment, DMZ, or internal network
- Encryption using a safe encryption algorithm when storing specific Personal Data of End Users (Unique Identification Data, credit card number, bank account number and biometric data)
- Encryption using a safe encryption algorithm when storing Personal Data of End Users and Unique Identification Data or biometric data of Data Subjects who are not End Users in users' PC, mobile device or supplementary storage device
- Procedures for secure generation, usage, storage, and distribution of encryption keys to safely store encrypted Personal Data

10. Destruction of data

Any of following measures should be put in place to destroy data pursuant to Clause 7(c) of this Agreement:

- Complete destruction (incineration, shredding, etc.)
- Deletion using specialized degaussing device
- Initialization or overwriting so that the data cannot be restored
- (In cases where only a part of the data is destroyed) for electronic files, management and supervision of files to ensure that Personal Data cannot be recovered or reproduced after deletion; for other records, deletion of the relevant parts by masking, perforating, etc.
- (In cases where it is difficult to destroy the data using the above methods due to technical characteristics) measures for processing it as anonymized information to make recovery impossible

11. Establishment and implementation of an internal privacy regulation

Internal privacy regulations shall be established and implemented. These include:

- Establishment and implementation of an internal privacy regulation through internal decision making procedures in order to prevent the loss, theft, leakage, forgery, or fabrication of Personal Data
- In the event of material changes to any of the items of the internal privacy regulation, immediately updating it to reflect such changes and maintaining records of any changes made
- Assessment and management of the implementation status of the internal privacy regulation (e.g. management of access authority, storage and inspection of access records, encryption measures) by the officer responsible for its privacy compliance at least once a year

Annex III: List of subprocessors

https://www.softbank.jp/privacy/contact/gdpr/

Annex IV: California Consumer Privacy Act (CCPA) instructions

These instructions (these “CCPA Instructions”) are provided to SoftBank as documented instructions of the customer under Article 4.2 of this Agreement.

In accordance with Article 4.2(a) of this Agreement, SoftBank must additionally comply with these CCPA Instructions to the extent that (i) SoftBank will Process the Personal Information of any California Consumers, or (ii) any Personal Data Processed by SoftBank pursuant to this Agreement is otherwise within the scope of the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 et seq.) as amended by the California Privacy Rights Act of 2020, and its implementing regulations (collectively, the “CCPA”).

In these CCPA Instructions, “Business,” “Consumer,” “Contractor,” “Cross-context behavioral advertising,” “Personal Information,” and “Service Provider” have the meanings given to those terms in the CCPA, and any other capitalized terms have the meanings ascribed to them in this Agreement. Also, the customer and SoftBank acknowledge that, as to the Processing of Personal Information, the customer will act as a Business and SoftBank will act as its Service Provider or Contractor.

The Customer’s Instructions to SoftBank

1. SoftBank must not (i) retain, use, or disclose Personal Information outside of its direct business relationship with the customer or for any commercial purpose other than to provide the services specified in the Terms of Use or as otherwise permitted by the CCPA, or (ii) combine the Personal Information with Personal Information that SoftBank has received from a source other than the customer or collected from a Consumer except for the case that SoftBank performs any business purpose as permitted under the CCPA.

2. SoftBank must not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, the Personal Information to third parties for monetary or other valuable consideration.

3. SoftBank must not share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, the Personal Information to third parties for Cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

Certification

By entering into this Agreement, SoftBank certifies that it understands its obligations under the CCPA and will comply with this Agreement and these CCPA Instructions.