Kawamura International Co., Ltd. Data Processing Addendum

Revision History

Version	Date	Summary of Major Changes
First Edition	2026-09-07	Published as the First Edition

Part I: General Provisions

Article 1 (Definitions)

In this Addendum, the meanings of the terms set forth in the following items shall be as prescribed in the respective items. Terms not defined in this Addendum shall have the meanings set forth in the Terms of Use for the Applicable Services.

1. "**Company**" means Kawamura International Co., Ltd.
2. "**Customer**" means a corporation, other organization, or sole proprietor that has entered into a contract with Company for the use of the Applicable Services.
3. "**Applicable Services**" means the services listed in Appendix 1.
4. "**Target Data**" means data transmitted by Customer to the Applicable Services.
5. "**Personal Information Protection Act**" means the Personal Information Protection Act (Act No. 57 of 2003).
6. "**Personal Data**" means personal data as defined in Article 16, paragraph 3 of the Personal Information Protection Act that is included in the Target Data and, where Appendix A applies, includes personal data as defined in Article 4(1) of the GDPR.
7. "**GDPR**" means Regulation (EU) 2016/679.
8. "**Sub-processor**" means a third party to which Company subcontracts part of the handling of Personal Data.
9. "**Supplementary Rules**" means the "Supplementary Rules on the Handling of Personal Data Transferred from the EU and the UK Based on an Adequacy Decision under the Personal Information Protection Act," established by the Personal Information Protection Commission.
10. "**Data Subject**" means an individual identified by personal data.

Article 2 (Scope of Application and Roles of the Parties)

1. This Addendum applies where the Target Data includes personal data.
2. Customer is the person who entrusts the handling of personal data (or, where Appendix A applies, the controller) and Customer determines the purposes and means of such handling. Company is the person entrusted by Customer with the handling of personal data (or, where Appendix A applies, the

processor).

3. The scope of personal data that Customer may transmit to the Applicable Services is governed by the AUP and other provisions applicable to such Applicable Services. **Customer shall not transmit special care-required personal information (except for information subject to the proviso to Article 15, paragraph 2) , shall limit the personal information transmitted to the minimum necessary, and shall, where possible, process it so that the Data Subject cannot be identified before transmitting it.**

4. In the event of any conflict between the provisions of this Addendum and the Terms of Use of the Applicable Services, this Addendum shall prevail with respect to matters concerning the handling of personal data.

5. In the event of any conflict between the common terms of this Addendum and the provisions of an Appendix, that Appendix shall prevail to the extent that it applies.

Article 3 (Details of Processing)

The purpose and nature of the processing of personal data, the types of personal data, the categories of data subjects, and the duration and location of processing shall be as set forth in Appendix 2.

Article 4 (Processing Based on Instructions)

1. Company will process personal data in accordance with this Addendum, the Terms of Use for the Applicable Services, and Customer's instructions, and Company will not process it beyond the scope thereof.

2. Company will not use personal data for purposes other than providing the Applicable Services and fulfilling the obligations set forth in this Addendum. Company will not use personal data to train or further train machine learning models.

3. If Company determines that Customer's instructions violate applicable laws and regulations, Company will immediately notify Customer. In such case, Company may suspend the performance of such instructions.

4. Customer's instructions include those given through the functions of the Applicable Services. Any instructions beyond the scope of the functions of the Applicable Services shall be separately agreed upon by Company and Customer.

Article 5 (Supervision of Employees)

1. Company shall limit the employees who handle personal data to the minimum necessary and impose confidentiality obligations on such employees.

2. Company shall regularly provide such employees with training on the proper handling of Personal Data.

3. Company shall provide necessary and appropriate supervision over such employees' handling of personal data.

Article 6 (Security Management Measures)

1. Company shall implement the security management measures set forth in Appendix 4 to prevent the leakage, loss, or damage of Personal Data.

2. Company shall continuously review the security management measures in light of technological advances, changes in threats, and other circumstances. Company shall maintain security management measures at a level equivalent to or higher than the level at the time of execution of this Addendum.

3. Company has obtained Privacy Mark certification for its personal information protection management system (Certification No. 10840770).

Article 7 (Confidentiality)

1. Company will keep personal data confidential and Company will not disclose it to third parties except as provided in this Addendum.

2. If Company is required by law or by a request from a competent authority to disclose personal data, Company will notify Customer in advance unless prohibited by law.

Article 8 (Sub-processors)

1. Customer agrees in advance that Company may entrust the handling of personal data to the sub-processors listed in Appendix 3.

2. Company will select sub-processors based on Company's selection criteria and enter into agreements with such sub-processors that impose obligations equivalent to or greater than Company's obligations set forth in this Addendum (including matters concerning security management, subcontracting, reporting on the status of handling, and reporting and notification in the event of an incident or accident) that impose such obligations. (Such agreements include arrangements under which Company agrees to the data processing terms, terms of use, or other terms prescribed by the relevant sub-processors.)

3. Company will periodically review the status of personal data handling by sub-processors.

4. Company is responsible to Customer for the performance of obligations by sub-processors.

5. Changes to Sub-processors. If Company adds or changes a sub-processor, Company will notify Customer at least 30 days before the Effective Date (or, if the period from the date on which Company receives notice of such addition or change from the sub-processor to the Effective Date is less than 30 days, promptly after receiving such notice). Customer may object to such addition or change on reasonable grounds. If the matter is not resolved through consultation between Company and Customer, Customer may terminate the Service Agreement for the services using the relevant sub-processor before the Effective Date. In this case, Company will refund, on a prorated basis, the portion of the monthly fees already paid for the relevant services corresponding to the period from the date of termination until the expiration date of the applicable Usage Period (this will be handled in the same manner as Article 17, Paragraph 7, Item 2 of the LDX hub Terms of Use).

6. The most current list of sub-processors shall be as set forth in Appendix 3.

Article 9 (Provision to Third Parties Located in Foreign Countries)

1. If Company provides Personal Data to a sub-processor located in a foreign country, the name of the sub-processor, the country in which it is located, and the legal basis for the cross-border transfer shall be stated in the “Third Parties Located in Foreign Countries” column of Appendix 3. This Article shall not apply to the provision of data to business operators listed in the “Domestic Contractors” column of Appendix 3.

2. Except where the relevant foreign country is a country designated by the Personal Information Protection Commission pursuant to Article 28, paragraph (1) of the Personal Information Protection Act, Company shall establish a system that complies with the standards prescribed in Article 16 of the Ordinance for Enforcement of the Personal Information Protection Act by ensuring, through appropriate and reasonable methods, that the relevant sub-processor implements measures consistent with the purpose of the provisions of Chapter IV, Section 2 of the Personal Information Protection Act with respect to its handling of Personal Data. Such methods include, in addition to entering into an individual contract with the relevant sub-processor, establishing binding arrangements by agreeing to data processing terms, terms of use, or other conditions established by the relevant sub-processor.

3. Company shall, at least once a year, periodically verify, through appropriate and reasonable methods, the status of the relevant sub-processor's implementation of the equivalent measures referred to in the preceding paragraph and the existence and content of systems for the protection of personal information in the relevant foreign country, and shall keep records of the results.

4. If any impediment arises to the implementation of the equivalent measures, Company shall take necessary and appropriate measures and, if it is difficult to eliminate the impediment, shall cease providing personal data to the relevant sub-processor. In such case, Company shall notify Customer without delay.

5. Company shall provide the following information at the request of the data subject. If a request from the data subject is made directly to Company, Company shall forward it to Customer.

   (1) Name of the relevant foreign country

   (2) Information concerning systems for the protection of personal information in the relevant foreign country

   (3) An outline of the equivalent measures to be taken by the relevant sub-processor

   (4) Method and frequency of confirmation under Paragraph 3

   (5) The existence and details of any impediment to the implementation of the Equivalent Measures, and the measures taken by Company in response thereto

6. **Appendix C shall apply to Personal Data transferred from within the EU and the UK pursuant to an adequacy decision, and Appendix C-4 shall prevail over this Article.** When Customer transmits such Personal Data to the Applicable Services, Customer shall notify Company thereof in advance.

Article 10 (Cooperation in the Exercise of Rights by the Data Subject)

1. Customer shall handle requests from the Data Subject for disclosure, correction, addition, deletion, suspension of use, erasure, suspension of provision to third parties, and other requests.

2. Company shall, to a reasonable extent, provide the cooperation necessary for Customer to take the measures set forth in the preceding paragraph.

3. If Company receives a request directly from the Data Subject, Company shall not respond to such request itself and shall promptly forward it to Customer. However, this shall not apply where Company is required by law to respond directly.

Article 11 (Response in the Event of a Data Breach, etc.)

1. Company will notify Customer without delay and within 72 hours of becoming aware of any leakage, loss, damage, or other incident involving personal data. If such an incident occurs at a sub-processor, the 72-hour period shall commence when Company receives notice from the sub-processor.

2. The notification referred to in the preceding paragraph shall include, to the extent known, an overview of the incident; the categories of personal data concerned and the number of Data Subjects; the cause; whether there has been, or there is a risk of, secondary harm and the details thereof; the status of measures taken in respect of Data Subjects; the status of public disclosure; measures to prevent recurrence; and Company's contact information.

3. The report to the Personal Information Protection Commission and notification to the data subject as prescribed in Article 26 of the Personal Information Protection Act shall be made by Customer. Company will provide Customer with the information necessary for Customer to do so.

4. Company will immediately take the measures necessary to prevent the incident from escalating and to investigate its cause.

Article 12 (Reporting and Confirmation of Handling Status)

1. At Customer's request, Company will report on the status of its handling of personal data, using the form prescribed by Company, no more than once per year.

2. Company will provide Customer with the information necessary for Customer to verify compliance with this Addendum. Company will obtain audit reports or certifications from third parties (including the PrivacyMark and ISO/IEC 27001). Customer may comply with such confirmation by providing materials relating thereto.

3. If there are reasonable grounds why confirmation under the preceding paragraph is insufficient, Company and Customer may separately agree to conduct an audit at Company's place of business. The scope, method, timing, and allocation of costs for the audit shall be determined by such agreement.

4. When conducting an audit, Customer shall permit entry only to persons who are subject to confidentiality obligations with respect to Company's Confidential Information.

Article 13 (Measures Where Compliance with the Terms of this Addendum Is Not Confirmed)

1. If Company is found to be in breach of this Addendum, Company shall, at Customer's request, submit and implement a remediation plan.

2. If the remediation referred to in the preceding paragraph is not carried out, Customer may terminate the agreement for use of the Applicable Services.

3. If a sub-processor is found to have breached its obligations under Article 8, Paragraph 2 of this Addendum, Company shall request that sub-processor to remedy the breach and, if the breach is not remedied, cease providing personal data to that sub-processor.

Article 14 (Retention Period and Deletion)

1. Company shall not retain personal data beyond the period specified in Appendix 2. After the expiration of the relevant period, Company will delete it.

2. Uploaded documents and output files will be automatically deleted three days after upload. If Customer wishes to request deletion before the expiration of the relevant period, Customer shall contact Company at privacy@k-intl.co.jp. **Company does not provide an endpoint for deletion.**

3. **Access in lieu of return.** The personal data held by Company is contained in the documents Customer uploads and the output already returned to Customer by Company, and is not data held solely by Company. During the period specified in the preceding paragraph, Customer may obtain the relevant data using the file function. Company and Customer confirm that this constitutes fulfillment of the return obligation set forth in Article 28(3)(g) of the GDPR.

4. If the agreement for use of the Applicable Services terminates, Company will delete the Personal Data upon expiration of the period specified in Appendix 2. **Because documents and output files are deleted after three days, no separate retrieval period will be provided after termination of the agreement.**

5. Execution logs shall be retained for the period required by the Corporation Tax Act and other laws and regulations (seven years. If laws and regulations require retention for a longer period, they shall be retained for such period). Execution logs do not include the contents of documents, the contents of outputs, or file names.

6. File names shall be replaced with SHA-512 hash values upon expiration of the period specified in Paragraph 2. Such replacement is based on deterministic hashing and does not constitute the creation of anonymously processed information.

7. Backups. Company regularly creates backups. The maximum period required for deleted Personal Data to be removed from backups is eight days. During such period, the provisions of this Addendum shall continue to apply to such Personal Data, and Company will not use it for restoration or any other purpose. Backups are stored in the Tokyo Region of Amazon S3 and are not replicated to other Regions. As versioning is not used, deletion entails actual deletion.

8. At Customer's request, Company may provide a bulk export in a format Company maintains. In this case, the format, method of provision, deadline, and fee shall be separately agreed upon by Company and Customer.

9. At Customer's request, Company will certify in writing, to a reasonable extent, that deletion has been carried out.

Article 15 (Customer Obligations and Representations)

1. Customer represents and warrants each of the following:

   (1) Customer has lawfully obtained the Personal Data, and transmission to the applicable service is within the scope of the purpose of use specified at the time of such acquisition.

   (2) Customer has a legally required basis for transmission to the Applicable Services and for processing by Company and its sub-processors under this Addendum.

   (3) Customer has provided the Data Subjects with any required notice or made any required public announcement.

   (4) Where transmission to the applicable service requires consent or other procedures under Article 27 or Article 28 of the Personal Information Protection Act, Customer has completed such procedures.

2. Customer shall not transmit any Special Care-Required Personal Information to the Applicable Services. However, if the AUP for the Applicable Services provides for a proviso concerning information processed so that the Data Subject cannot be identified, the provisions of such proviso shall apply. With respect to the LDX hub, pursuant to the proviso to Article 3, Paragraph 1 and the provisions of Paragraph 2 of the same Article of the AUP, Customer may transmit information processed so that the Data Subject cannot be identified, excluding pseudonymously processed information obtained by processing personal information transferred from the EU or the UK pursuant to an adequacy decision.

3. Customer shall limit the personal data transmitted to the Applicable Services to the minimum necessary and, where possible, process it so that the Data Subject cannot be identified before transmitting it.

4. If Company suffers any damage as a result of Customer's breach of the preceding three paragraphs, Customer shall compensate Company for such damage.

Article 16 (Data Protection Impact Assessment and Prior Consultation)

If Customer conducts an impact assessment regarding the handling of personal data or engages in prior consultation with a supervisory authority, Company shall provide reasonable cooperation to the extent of the information it possesses.

Article 17 (Liability)

1. The limitations on damages set forth in the Terms of Use for the Applicable Services shall apply to Company's liability under this Addendum.

2. Notwithstanding the preceding paragraph, where Appendix A applies, the GDPR and other applicable laws and regulations shall prevail to the extent that they do not permit limitations of liability.

Article 18 (Term and Termination)

1. This Addendum shall remain in effect for as long as the agreement for the use of the Applicable Services remains in effect.

2. Articles 7, 10, paragraphs 3, 11, 14, and 17 shall remain in effect after the termination of this Addendum for as long as Company retains the personal data. Article 14, paragraph 5 shall remain in effect until the expiration of the statutory retention period, and paragraph 7 of the same Article shall remain in effect until the personal data is deleted from backups.

Article 19 (Amendmentss)

1. Company may amend this Addendum due to changes in laws and regulations, changes in the views of supervisory authorities, changes in sub-processors, or other circumstances.

2. The amendments referred to in the preceding paragraph shall be made in accordance with the procedures for amendments set forth in the Terms of Use for the Applicable Services. However, for amendments that reduce Customer's rights, Company shall provide notice at least 30 days before the effective date, and Customer may terminate the Service Agreement before the effective date.

3. Any amendment to this Addendum entered into separately shall require the written agreement of Company and Customer.

Article 20 (Governing Law)

This Addendum shall be governed by the laws of Japan. However, each of Appendices A through D shall, to the extent it concerns the interpretation of the laws and regulations to which such Appendix corresponds, be governed by such laws and regulations.

Appendix 1: Applicable Services

Services	Effective Date	Conditions for Application	Remarks
LDX hub (StructFlow, AnalyzeDoc, RefineLoop, RenderOCR, CastDoc, ExtractDoc, file functionality, MCP endpoints)	September 7, 2026	Applicable as Part of the Terms of Use	Not applicable to TermFit, QualScope, TM Builder, and Style Guide Builder

Appendix 2: Details of Processing

Item	Details
Purpose of Handling	Provision of the Applicable Services. Namely, document and text translation, translation refinement, structured data extraction, optical character recognition, document format conversion, terminology processing, and translation quality measurement
Nature of Handling	Automated processing. Access to content by Company's employees shall be limited to the minimum extent necessary and only when necessary to investigate incidents, respond to Customer inquiries, or comply with laws and regulations. **However, when processing is performed using an Azure OpenAI Service model, Microsoft Japan Co., Ltd. shall retain prompts and outputs for 30 days for misuse monitoring and subject them to review by its personnel. Company cannot use settings to avoid this.** This handling will not occur if Customer does not specify the relevant model.
Types of Personal Data	Names, titles, affiliations, employers, contact information (email addresses, telephone numbers, and addresses), and signatures included in business documents. File names may contain Personal Information, but are replaced with hash values after three days. No special care-required Personal Information is included (Article 15, Paragraph 2). However, pursuant to the proviso to the same paragraph, data processed so that the individual cannot

Item	Details
	be identified (data subject to the proviso to Article 3, Paragraph 1, and Article 3, Paragraph 2, of the AUP) may be transmitted, in which case the processed data will be subject to handling.
Categories of Data Subjects	Officers and employees of Customer, officers and employees of Customer's business partners, parties to contracts, and other individuals appearing in documents processed by Customer
Retention Period	(1) Uploaded documents and output files: Three days from upload (automatically deleted based on expires_at). (2) Data returned by the API as a result of job execution: Not retained. (3) Execution logs: Seven years (as they include billing aggregation records and constitute legally required books and documents). Do not include document contents or file names. (4) File names: Replaced with a SHA-512 hash value upon expiration of the period in (1). The size and the creation and expiration dates and times are the same as in (3).
Place of Processing	**Documents and execution logs are stored in Japan** (Tokyo Region of Amazon Web Services Japan LLC). For processing by third-party models, the countries in which the sub-processors listed in Appendix 3 are located. **For both Amazon Bedrock and Azure OpenAI Service, global inference configurations are used; therefore, inference processing may be performed in regions outside Japan.** (Appendix 4)

Appendix 3: Sub-processors

Domestic contractors (not constituting provision to third parties in foreign countries)

Name	Location	Details of Handling	Target Services
Amazon Web Services Japan G.K.	Japan (Tokyo Region)	Hosting, file storage, execution log storage, and generative processing of text using Amazon Bedrock	All
Microsoft Japan Corporation	Japan (Tokyo Region. However, inference processing is as follows.)	Generative processing of text using Azure OpenAI Service. For the purpose of monitoring for misuse, prompts and outputs are retained for 30 days and are subject to review by	StructFlow, RefineLoop, AnalyzeDoc

Name	Location	Details of Handling	Target Services
		its personnel (Appendix 2).	

Third Party in a Foreign Country (System for Ensuring Compliance with the Standards under Article 16 of the Enforcement Regulations)

Name	Country of Location	Details of Handling	Applicable Services	Basis for Cross-Border Transfer
OpenAI	United States	Generative Processing of Text	StructFlow, RefineLoop, AnalyzeDoc	Article 16 of the Enforcement Regulations
Google	United States	Generative processing of text. Because Customer has enabled its Cloud Billing account, Google will treat this as a paid service and will not use prompts and responses to improve the product.	StructFlow, RefineLoop, AnalyzeDoc	Article 16 of the Enforcement Regulations
Anthropic	United States	Generative Processing of Text	StructFlow, RefineLoop, AnalyzeDoc	Article 16 of the Enforcement Regulations
SpaceXAI (formerly xAI)	United States	Generative Processing of Text	StructFlow, RefineLoop	Article 16 of the Enforcement Regulations
Zuplo, Inc.	United States	API gateway (authentication, billing metering, rate limiting, header addition, and request forwarding). Request and response bodies and headers (excluding tracing headers) are not collected. The information collected includes URLs and routes, HTTP methods, status codes, response times, request and	All	Article 16 of the Enforcement Regulations

Name	Country of Location	Details of Handling	Applicable Services	Basis for Cross-Border Transfer
		response lengths, API key identifiers, user agents, IP addresses, geographic information, and tracing headers.		

RenderOCR, CastDoc, and ExtractDoc are processed by Company's engines (KI OCR, KI Cast, and KI Extract) and are not provided to third parties located in foreign countries.

Appendix 4: Security Control Measures

Category	Details of Measures
Organizational Security Control Measures	Operation of the Personal Information Protection Management System (PrivacyMark). Appointment of a personal information protection manager and a personal information protection audit manager. Maintenance of a personal information management register and a contractor management register. Conducting internal audits. Establishment of a reporting system in the event of incidents or accidents.
Personnel Security Measures	Execution of confidentiality agreements with employees. Provision of regular training. Limiting handling authority to the minimum necessary level.
Physical Security Control Measures	Control of entry to and exit from business premises. Management of equipment and media containing personal data (including restrictions on their removal and erasure of data upon disposal). Establishment of internal rules governing the handling of work terminals and documents.
Technical Security Management Measures	Access control and authentication (authentication using API keys and access rights management). Encryption of communications (TLS). Encryption at rest. Collection and retention of access logs. Vulnerability management
Understanding the External Environment	Ascertain and record the legal framework for the protection of personal information in the countries where the sub-processors listed in Appendix 3 are located. Understand the range of regions in which inference processing may be performed under a configuration using Amazon Bedrock's global inference profiles and Azure OpenAI Service's global standard deployment, whereby such processing may occur in regions outside the country. Review the list of

Category	Details of Measures
	sub-processors published by the sub-processor. Review at least once a year
Certification	PrivacyMark (JIS Q 15001), ISO/IEC 27001

Appendix A: Additional Provisions for the EU and EEA (GDPR)

This Appendix applies where Customer is subject to the GDPR.

A-1 Definitions

In this Appendix, the terms "controller," "processor," "processing," "personal data," and "supervisory authority" have the meanings set forth in Article 4 of the GDPR. Customer is the controller, and Company is the processor.

A-2 Provisions corresponding to Article 28(3) of the GDPR

Article 28(3) of the GDPR	Corresponding provisions of this Addendum
(a) Processing based on documented instructions (including cross-border transfers)	Article 4, Article 9
(b) Confidentiality of employees	Article 5, Article 7
(c) Security measures under Article 32	Article 6, Appendix 4
(d) conditions relating to sub-processors (Article 28(2) and (4))	Article 8
(e) cooperation in the exercise of rights by data subjects (Chapter 3)	Article 10
(f) cooperation in complying with Articles 32 to 36	Articles 6, 11 and 16
(g) deletion or return upon termination	Article 14 (pursuant to paragraph 3, return shall be effected by downloading through the file function)
(h) provision of information necessary to demonstrate compliance and cooperation with audits	Article 12
Notice Where Instructions Violate Laws and Regulations	Article 4, Paragraph 3

A-3 Transfers from the EU and Adequacy Decision

1. Japan has received an adequacy decision from the European Commission pursuant to Article 45 of the GDPR, and that decision remains in effect. Therefore, the transfer of personal data from Customer to Company does not require standard contractual clauses or any other transfer mechanism provided for in Article 46 of the GDPR.
2. Notwithstanding the preceding paragraph, if Customer requests that standard contractual clauses be entered into, Customer and Company may enter into such clauses following separate consultation.

3. Article 9 and Appendix C shall apply to onward transfers from Company to sub-processors located in foreign countries.

A-4 Rights of Data Subjects

1. If Company receives a direct request from a data subject to exercise their rights, Company shall not respond to it directly and shall promptly refer the request to Customer.

2. Company shall cooperate by implementing technical and organizational measures necessary for Customer to fulfill Customer's obligations under Articles 12 through 22 of the GDPR.

A-5 Notice of Infringement

The notification set forth in Article 11, Paragraph 1 shall also be made in fulfillment of the processor's obligations under Article 33(2) of the GDPR.

Appendix B Additional Provisions for the United Kingdom

This Appendix applies where Customer is subject to UK data protection law.

1. The provisions of Appendix A shall apply, with "GDPR" read as "UK GDPR" and "supervisory authority" read as "Information Commissioner (ICO)".

2. A framework for the smooth mutual transfer of personal data between Japan and the United Kingdom remains in place, and the data protection regimes of both are considered equivalent. Accordingly, no International Data Transfer Agreement or International Data Transfer Addendum is required for transfers from Customer to Company.

3. If Customer requests that an International Data Transfer Addendum be entered into, Company and Customer may enter into it.

Appendix C Supplementary Rules (Personal Data Transferred from within the EU or the United Kingdom Based on an Adequacy Decision)

This Appendix applies where Customer transmits to the Applicable Services personal data received by Customer from within the EU or the United Kingdom pursuant to an adequacy decision. This Appendix corresponds to the "Supplementary Rules on the Handling of Personal Data Transferred from the EU and the UK Based on an Adequacy Decision under the Act on the Protection of Personal Information" (established in January 2019 and partially amended in December 2023; hereinafter referred to as the "Supplementary Rules") prescribed by the Personal Information Protection Commission.

C-1 Prerequisites for Application

1. If Customer transmits to the Applicable Services personal data transferred from the EU or the UK pursuant to an adequacy decision, Customer shall notify Company thereof in advance. Such notification may be made by email or any other method specified by Company and need not be made through the input fields in the Applicable Services.

2. In addition to the Personal Information Protection Act, Company shall handle personal data for which

it has received notification under the preceding paragraph in accordance with the Supplementary Rules.

3. Company shall record and manage in its vendor management ledger and other internal records the fact that it received the notification under the preceding paragraph, the relevant customer, and the scope of the Target Data. Because Company cannot determine the origin of a transmitted document from its content, this Appendix applies based on notification by Customer.

C-2 Special Care-Required Personal Information

1. Information that should be treated as special care-required personal information under the supplementary rules (including information concerning sexual life, sexual orientation, and labor unions, which are defined as special categories of personal data under the GDPR and the UK GDPR) Article 15, paragraph 2 of this Addendum shall apply, and Customer shall not transmit it (except where the proviso to that paragraph applies). However, pseudonymously processed information obtained by processing personal data to which this Appendix applies may not be transmitted pursuant to C-5, Paragraph 2.) . To avoid the need to determine the origin, Company applies the restrictions in this paragraph uniformly to all Subject Data, rather than limiting them to personal data to which this Appendix applies. This treatment is reflected in Article 3, Paragraph 1 of the LDX hub AUP.

2. Company shall impose on Sub-processors the same restrictions as those set forth in the preceding paragraph.

C-3 Specification and Limitation of Purposes of Use

1. Company shall confirm and record the circumstances of acquisition of personal data to which this Appendix applies, including the purpose of use specified when such personal data is received from Customer.

2. Company shall specify the purposes of use within the scope of the purposes of use recorded pursuant to the preceding paragraph and handle such personal data within that scope.

C-4 Re-transfer to a Third Party in a Foreign Country

1. When Company provides personal data to which this Appendix applies to a third party located in a foreign country, it must obtain the prior consent of the Data Subject to such provision, unless any of the following applies.

   (1) Where the third party is located in a country designated by the Personal Information Protection Commission (the EU, the UK, or another designated country)

   (2) Where Company and the third party have jointly implemented measures for the protection of personal information at a level equivalent to that under the Personal Information Protection Act, including supplementary rules, by appropriate and reasonable means (such as a contract, another form of binding arrangement, or binding rules within a corporate group) with respect to the third party's handling of personal data

   (3) Where any of the items of Article 27, paragraph 1 of the Personal Information Protection Act applies

2. Company will carry out onward transfers by the method set forth in item (2) of the preceding paragraph. In this case, Company shall ensure, in its contract with the sub-processor, the implementation of the measures listed in the following items, in addition to the matters set forth in Article 9 of this Addendum.

(1) Restrictions on special care-required personal information set forth in C-2

(2) Restrictions on the purposes of use set forth in C-3

(3) Restrictions on pseudonymously processed information set forth in C-5

(4) Restrictions on anonymously processed information set forth in C-6

(5) Measures equivalent to those set forth in this Appendix in the event that the relevant sub-processor makes a further onward transfer

3. Company will not provide personal data to which this Appendix applies to any sub-processor that cannot ensure the implementation of the measures set forth in the preceding paragraph. In this case, the processing of the relevant personal data will be limited to sub-processors falling under Item 1 of Paragraph 1.

4. In the case set forth in the preceding paragraph, Company will, upon Customer's request, notify Customer of the sub-processors that may be used for the relevant processing.

C-5 Pseudonymously Processed Information

1. Company will not create pseudonymously processed information by processing personal data to which this Appendix applies.

2. Customer may not transmit to the Applicable Services any pseudonymously processed information obtained by processing Personal Data to which this Appendix applies.

C-6 Anonymously Processed Information

Company will not create anonymously processed information from Personal Data to which this Appendix applies. Processing shall be carried out by Customer (Article 15, paragraph 3 of this Addendum). In addition, the Supplementary Rules provide that Personal Information to which this Appendix applies shall be deemed anonymously processed information only if it has been made impossible for anyone to re-identify an individual anonymized by deleting information concerning the methods of processing, etc.

C-7 Publication of Matters Concerning Retained Personal Data

Company will publish, at https://www.k-intl.co.jp/privacy_policy, the matters required by the Supplementary Rules with respect to personal data to which this Appendix applies.

C-8 Enforcement

The Supplementary Rules are legally binding rules, and if Company fails to comply with the obligations set forth therein, the Personal Information Protection Commission has the authority to take measures pursuant to Article 148 of the Personal Information Protection Act.

Appendix D Additional Provisions for the United States (CCPA/CPRA)

This Appendix applies if Customer is subject to the California Consumer Privacy Act (CCPA), as amended by the CPRA.

1. Company handles Personal Information as a "service provider" as defined in the CCPA. Company is

not a "third party".

2. Company will process Personal Information solely for the purpose of fulfilling the business purposes set forth in the contract with Customer and will not engage in the following activities:

   (1) sell or share Personal Information;

   (2) retain, use, or disclose Personal Information for purposes other than those set forth in the contract;

   (3) combine Personal Information obtained from Customer with Personal Information obtained from other sources, except as permitted by the CCPA;

   (4) use Personal Information for Company's own commercial purposes.

3. Company will comply with the obligations set forth in the CCPA and provide the cooperation necessary for Customer to comply with the CCPA.

4. Company will impose on sub-processors obligations equivalent to those set forth in this Appendix.

5. Company will immediately notify Customer if Company becomes unable to perform the obligations set forth in this Appendix.

6. Customer has the right to take reasonable and appropriate measures to stop and remedy Company's handling of personal information in violation of the CCPA.