Data Processing Agreement

This Data Processing Agreement (including any appendices and exhibits, the "DPA") applies in connection with the use by the Customer (the "Controller") of copyrighted works licensed to the Controller by Nikon Corporation (the "Processor") under the End-User License Agreement (the "Original Agreement"). The Processor will process personal data on behalf of the Controller in connection with such use. This DPA forms part of the Original Agreement, and the Controller's consent to the Original Agreement shall be deemed consent to this DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of this DPA is to ensure compliance with applicable data protection laws and regulations, including without limitation, Japan's Act on the Protection of Personal Information (Act No. 57 of May 30, 2003) and as amended ("**Japan's APPI**") ("**Data Protection Laws and Regulations**"). This DPA is a special provision of the Original Agreement. If there are any points not stipulated in this DPA, the provisions of the Original Agreement shall be applicable. In addition, if there are any conflicts between the Original Agreement and this DPA, the provisions of this DPA shall prevail.

(b) This DPA applies to the processing of personal data as specified in Appendix I.

(c) This DPA is without prejudice to obligations to which the Controller is subject by virtue of applicable Data Protection Laws and Regulations.

Clause 2

Interpretation and Definition

(a) Where this DPA uses the terms defined in the EU General Data Protection Regulation (Regulation (EU) 2016/679, as amended from time to time) (the "GDPR") but not defined in this DPA, those terms shall have the same meaning as in the GDPR.

(b) This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in applicable Data Protection Laws and Regulations or in a way that prejudices the fundamental rights or freedoms of the data subjects.

(c) For the purposes of this DPA, the following definitions apply:

(1) **"Parties"** means the Controller and the Processor collectively.

(2) **"Party"** means either the Controller or the Processor individually.

(3) **"Foreign Country"** means a foreign country from the perspective of Data Protection Laws and Regulations enacted by the legislative body of a country where the data subject or the Controller is located, such as a country where the data subject does not reside or a country where the Controller is not located; provided however, the EEA as a whole is deemed to be a single country for the purpose of "Foreign Country."

(4) "**International Transfer**" means a transfer to a Foreign Country.

(5) "**supervisory authority**" means one (or more) independent public authority(ies) which is (are) competent for the protection of the fundamentals rights and freedom of natural persons in relation to processing of personal data under the Regulations and Applicable Law, including Lead Supervisory Authorities as defined under the GDPR and any Attorney General or other governing authority under the US Data Privacy Laws.

Clause 3

Agreement Structure and Order of Priority

(a) In the event of any conflict or contradiction, unless explicitly specified otherwise elsewhere in this DPA, the following order of precedence shall apply and each Party shall comply with them in such order to the necessary extent:

(1) applicable Data Protection Laws and Regulations which provide greater protection for data subjects than provisions of (2), (3) and (4) below,

(2) Exhibit 1 ("**Country Specific Contractual Clauses**") of this DPA,

(3) this main body of this DPA,

(4) the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter.

(b) Exhibit 1 ("**Country Specific Contractual Clauses**") shall apply only to the processing activities which are subject to the Data Protection Laws and Regulations listed in these Exhibits. In case where Parties are subject to the Data Protection Laws and Regulations listed in Exhibit 1 ("**Country Specific Contractual Clauses**"), the Parties shall adhere to such Data Protection Laws and Regulations.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 4

Description of processing(s)

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 Controller, are specified in Appendix I.

Clause5

Obligations of the Parties

5.1. Instructions

(a) The Processor shall process personal data only on documented instructions from the Controller, unless required to do so by applicable Data Protection Laws and Regulations. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe applicable Data Protection Laws and Regulations.

5.2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Appendix I, unless it receives further instructions from the Controller.

5.3. Duration of the processing of personal data

Processing by the Processor shall only take place for the duration specified in Appendix I.

5.4. Security of processing

(a) The Processor shall implement the technical and organisational measures specified in Appendix II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties 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 involved for the data subjects.

(b) The Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor shall ensure that persons authorised to process the personal data

received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**sensitive data**"), the Processor shall apply specific restrictions and/or additional safeguards.

5.6 Documentation and compliance

(a) The Processor shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with this DPA.

(b) The Processor shall, if so requested by the Controller, provide the Controller with information necessary to demonstrate compliance with the obligations that are set out in the DPA or that stem directly from Data Protection Laws and Regulations. If, and only if, there are indications of non-compliance with the DPA by the Processor and the above provision of information is not sufficient to prove compliance with the DPA, then, not more than once a year (unless there is an urgent need), the Controller may, after giving the Processor written notice that indicates reasonable grounds (including via electromagnetic means; the same applies hereinafter) at least 30 business days for the Processor in advance, implement by itself or through a third-party auditor (limited to an auditor that is not a competitor of the Processor and for which the Processor's consent has been obtained; such consent must not be rejected by the Processor on unreasonable grounds), an on-site audit at the Processor during the Processor's ordinary business hours and within a scope that does not unduly obstruct the Processor's daily business and that does not breach contractual obligations with the Processor' s other contract parties. Prior to the commencement of the on-site audit, the Controller and the Processor must agree on the scope, timing, duration, confidentiality obligations, and the like related to the audit. The Controller shall bear the audit expense unless non-compliance with the DPA by the Processor is acknowledged or another separate agreement is reached in this regard.

5.7. Use of Sub-Processors

(a) The Processor has the Controller's general authorisation for the engagement of Sub-Processors (including Sub-Sub-Processors) from an agreed list which can be found in Annex III. The Processor shall specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of Sub-Processors at least 30 days in advance, thereby giving

the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned Sub-Processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

(b) Where the Processor engages a Sub-Processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the Sub-Processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with this DPA. The Processor shall ensure that the Sub-Processor complies with the obligations to which the Processor is subject pursuant to this DPA and to applicable Data Protection Laws and Regulations.

(c) The Processor will remain fully responsible to the Controller for the performance of the Sub-Processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the Sub-Processor to fulfil its contractual obligations.

5.8. International transfers

(a) Personal Data may be transferred to the following countries:

- Japan;
- The United States.

(b) If consent from the data subject is necessary under Data Protection Laws and Regulations in transferring personal data from the Processor to the Controller, on behalf of the Processor, the Controller shall obtain such consent from the data subject.

(c) Where each Party may require the other Party's co-operation, including the conclusion of a specific form of agreement, in order to comply with the international data transfer regulation, each Party shall notify the other Party in writing and the other Party shall co-operate with such request to the extent necessary and reasonable.

(d) International Transfers by the Processor

International Transfer of personal data by the Processor shall be carried out in compliance with applicable Data Protection Laws and Regulations, and such International Transfer may be carried out only on the basis of documented instructions from the Controller. For the avoidance of doubt, Clause 5.8(a) shall constitute such documented instructions.

Clause 6

Assistance to the Controller

(a) The Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the Controller.

(b) The Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the Processor shall comply with the Controller's instructions

(c) In addition to the Processor's obligation to assist the Controller pursuant to this Clause (b), the Processor shall furthermore assist the Controller in ensuring compliance with obligations under Data Protection Laws and Regulations, taking into account the nature of the data processing and the information available to the Processor:

(d) The Parties shall set out in Appendix II the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 7

Notification of personal data breach

In the event of a personal data breach, the Processor shall cooperate with and assist the Controller for the Controller to comply with its obligations to make data breach notification to the relevant authorities and data subjects in accordance with applicable Data Protection Laws and Regulations, where applicable, taking into account the nature of processing and the information available to the Processor.

7.1 Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Processor shall assist the Controller:

(a) in complying, pursuant to Data Protection Laws and Regulations applicable to the Controller, with the obligation to notify the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it;

(b) in obtaining the following information which, pursuant to Data Protection Laws and Regulations applicable to the Controller, shall be stated in the Controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information 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.

(c) in complying, pursuant to Data Protection Laws and Regulations applicable to the Controller, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

7.2 Data breach concerning data processed by the Processor

In the event of a personal data breach concerning data processed by the Processor, the Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information 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 8

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of applicable Data Protection Laws and Regulations, in the event that the Processor is in breach of its obligations under this DPA, the Controller may instruct the Processor to suspend the processing of personal data until the latter complies with this DPA or the Original Agreement is terminated. The Processor shall promptly inform the Controller in case it is unable to comply with this DPA, for whatever reason.

(b) Upon termination or expiration of the Original Agreement, or earlier at the Controller's request, the Processor shall, at the Controller's choice, either (i) return all Personal Data processed on

behalf of the Controller and delete all existing copies, or (ii) delete all Personal Data processed on behalf of the Controller, unless applicable Data Protection Laws and Regulations require retention of such Personal Data.

Clause 9

Governing Law and Jurisdiction

(a) This DPA is governed by the laws of Japan.

(b) Any disputes arising out of or in relation to this DPA shall be submitted to the exclusive jurisdiction of the Tokyo District Court, Japan.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

APPENDIX I: DESCRIPTION OF THE PROCESSING

Name and execution date of the Original Agreement (if applicable)	Name: End-User License Agreement Execution date: the same date as the Original Agreement
Categories of data subjects whose personal data is processed	Controller's employees
Categories of personal data processed	Personal data entered by the Controller's employees to designate file names for data stored on equipment supplied by the Processor in connection with the Original Agreement, including, without limitation, full name and email address.
Sensitive data processed (if applicable)	The Processor believes that categories of the personal data entrusted to the Processor by the Controller under the Original Agreement basically do not fall under the data defined as 「要配慮個人情報」 ("sensitive personal information") under Japan's APPI or as special categories of personal data under Article 9 of the GDPR.
Nature of the processing	The processing of personal data for the Processor's provision to the Controller of the services in accordance with the Original Agreement.
Purpose(s) for which the personal data is processed on behalf of the Controller	In order for the Controller to receive the services in accordance with the Original Agreement, and in order for the Processor to provide the Controller with such services. The Processor will process personal data contained in file names recorded on equipment in connection with the Original Agreement, and personal data contained in device operation logs generated when such files are executed, for the purposes of diagnosing equipment malfunctions, restoring systems following damage, and improving equipment, software, and services.
Duration of the processing (Retention period or criteria for retention)	The personal data will be processed and retained during the term of the Original Agreement.

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

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

Measures of pseudonymisation and encryption of personal data

- Personal data contained in file names and logs will not be pseudonymised or encrypted.

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

- The number of persons authorised to access personal data is limited to the minimum necessary, and the scope of such access is also limited to the minimum necessary.
- Backups are made on a regular basis.

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

- Periodic confirmation that the system can be recovered from backup data is carried out.

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

- The latest patches to operating systems and other software to reduce vulnerabilities is applied.

Measures for user identification and authorisation of the information system used for Processing

- The information system used for Processing is equipped with a user authentication function.

Measures for the protection of data during transmission

- When transmitting or taking personal data outside the Processor's office, personal data is encrypted.

Measures for the protection of data during storage

- Access control are in place when storing personal data.

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

- Processing of personal data takes place at a location within the Processor's office where access control is in place.

Measures for ensuring system configuration, including default configuration

- Configuration management is in place to develop information systems.

Measures for internal IT and IT security governance and management

- The Processor has established and operates a management system in accordance with the Information Security Management System (ISMS) under the commitment of the management team.

Measures for ensuring data minimisation

- The Processor designates its personnel with access privileges for each personal data based on the concept that personal data should be processed only by those who need them for the purpose of use.

Measures for ensuring data quality

- The Processor endeavours to keep personal data accurate and up-to-date, to the extent necessary to achieve the purpose of use.

Measures for ensuring limited data retention

- Personal data is promptly disposed of when no longer needed.

Measures for ensuring accountability

- The information management system (roles and responsibilities) is shown in the Processor's Information Management Rules, and information management Personnel are assigned to each department.

Training for the Processor's Personnel

- The Processor will periodically provide its personnel with training on points to keep in mind for processing personal data.

Exhibit 1 – Country Specific Contractual Clauses

Not applicable at present.