DATA PROCESSING ADDENDUM *(eMAINTENANCE -CANON (UK) LIMITED DIRECT CUSTOMER VERSION)*

This Data Processing Addendum ("**Data Processing Addendum**") forms part of and supplements the Contract entered into between Us and You governing Your use of the Online Services known as eMaintenance.

1. GENERAL

1.1. **Incorporation**: This Data Processing Addendum is in addition to and applies to the contractual relationship between Us and You and the terms set out herein are incorporated into the Contract.

1.2. **Conflict:** In case of a conflict between the terms of this Data Processing Addendum and the Contract, the terms of the Data Processing Addendum shall prevail to the extent of any inconsistency only.

1.3. **Definitions:** In this Data Processing Addendum, expressions defined in the Conditions and used in this Data Processing Addendum have the meaning set out in the Contract, where applicable, or are as set out in this Data Processing Addendum.

1.4. **Rules of Interpretation:** The rules of interpretation set out in the Conditions apply to this Data Processing Addendum.

2. SCOPE

2.1. This Data Processing Addendum shall apply to the processing of Customer Personal Data by Us pursuant to the Contract.

3. PROCESSING REQUIREMENTS

3.1. Unless otherwise set out in the Agreement or in Statements of Work or Purchase Orders submitted under the Contract, details about the Customer Personal Data to be processed by Us and the processing activities to be performed under this Data Processing Addendum are set out in Schedule 1.

3.2. We shall only process Customer Personal Data in accordance with the documented instructions given from time to time by You, including with regard to transfers, unless required to do so otherwise by applicable law. In which event, We shall inform You of the legal requirement before processing Customer Personal Data other than in accordance with Your instructions, unless that same law prohibits Us from doing so on important grounds of public interest.

3.3. Where You are also procuring the Services for one or more of Your Affiliates, You confirm that You are authorized to communicate any instruction or other requirements on behalf of such Affiliates to Us in respect of the Services.

3.4. If You are in breach of Your obligations under the Data Protection Legislation due to Our act or omission, We shall not be liable for such breach where such act or omission arose from Your instructions.

3.5. Upon termination or expiry of the Services, We shall, at Your request, promptly delete or return all Customer Personal Data and delete the copies thereof (unless applicable law requires the storage of such Customer Personal Data) and shall confirm to You in writing that We have done so. This is without prejudice to any provisions in the Contract relating to how long We may retain data after the Contract terminates. This is also without prejudice to Our rights to erase Customer Personal Data under clause 48.4 of the Conditions if You fail to provide such instruction within one month after termination of the Services.

4. SECURITY

4.1. We warrant and undertake in respect of all Customer Personal Data that We shall:

4.1.1. implement appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful processing against accidental loss, destruction, damage, alteration or disclosure, including such measures set out in Schedule 2 and as may be updated from time to time;

4.1.2. without prejudice to any general obligations relating to confidentiality in the Conditions, ensure that Our personnel are subject to binding obligations of confidentiality with respect to Customer Personal Data; and

4.1.3. promptly, and without delay, notify You in writing of any actual, alleged, or potential unauthorised disclosure, loss, destruction, compromise, damage, alteration, or theft of Customer Personal Data.

4.2. You shall promptly and without delay notify Us in writing if You become aware of any breach of security in respect of the Services or Your use of the Services.

5. ASSISTANCE

5.1. Taking into account the nature and scope of the Services provided by Us, We shall, to the extent possible, provide such assistance as You may reasonably require to comply with Your obligations as a data controller, including in relation to data security, data breach notification, data protection impact assessment, prior consultation with data protection authorities, any enquiry, notice or investigation received from a data protection authority, and the fulfilment of data subjects' rights.

5.2. We shall make available to You all information reasonably necessary to demonstrate Our compliance with the obligations set out in this Data Processing Addendum, and allow for and co-operate with any audits, including physical inspections of Our premises, required by You. You shall be limited to conducting one such audit or inspection per year, save where You reasonably believe that We may have breached the provisions of this Data Processing Addendum. Any such audit or inspection shall be conducted on reasonable notice during normal business hours. We may require that the people conducting the audit sign undertakings of confidentiality. Should the inspector appointed by You be in a competitive relationship with Us, We have a right of objection against them. The expenses incurred by Us for any such audit shall be borne by You.

6. SUB-PROCESSING

6.1. You provide Us with a general authorisation to appoint Sub-Processors to process the Customer Personal Data provided that You are: (i) informed of the identity of the Sub-Processor and are given reasonable notice of no less than 30 days in advance of any proposed changes concerning the addition or replacement of other Sub-Processors; (ii) given the opportunity to object to such changes where You consider that such Sub-Processors do not provide sufficient guarantees under Data Protection Legislation in which event We shall use reasonable endeavours to address Your concerns. If You fail to object within the 30 days' notice period, You will have been deemed to accept the appointment and/or replacement of the new sub-processor. You hereby authorise Us to use Sub-Processors: (i) expressly authorized in the Contract; (ii) listed in Schedule 3 of this Data Processing Addendum or (iii) that are Our Affiliates

6.2. We shall impose obligations on Our Sub-Processors that are equivalent to those set out in this Data Processing Addendum by way of written contract (including where Customer Personal Data may be processed outside the United Kingdom / European Economic Area), and We shall remain liable to You for any failure by a Sub-Processor to fulfil its obligations in relation to the Customer Personal Data.

7. DATA TRANSFERS

7.1. Where We appoint Sub-Processors in accordance with paragraph 6 above, We shall put in place terms with Our Sub-Processors to ensure that such Customer Personal Data is only processed in

accordance with Your instructions in connection with the Contract with You and shall include adequate safeguards which satisfy the requirements of the Data Protection Legislation (as defined in the Contract) in relation to any processing of Customer Personal Data that may be undertaken by Our Sub-Processors outside of the United Kingdom and/or European Economic Area. Such adequate measures may include:

7.1.1. processing in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or

7.1.2. appropriate safeguards to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Data Protection Legislation, including a transfer mechanism that enables compliance with cross-border data transfer provisions under applicable Data Protection Legislation.

8. LIABILITY

8.1. The provisions on the parties' liability contained in the Contract shall be valid also for the purposes of processing under this Data Processing Addendum, unless expressly agreed upon otherwise.

SCHEDULE 1

DESCRIPTION OF THE PERSONAL DATA PROCESSING

The data processing activities carried out by Us pursuant to the Contract and this Data Processing Addendum may be described as follows:

The data processing activities carried out by Canon pursuant to the Agreement and this DPA may be described as follows:

1. **Subject matter**

   eMaintenance (eM) is an efficient monitoring and diagnostic device management cloud application that provides remote support for all compatible Canon networked MFP/SFP devices. Easy to access via the cloud, it automates many of the time-consuming tasks related to managing the device. It can also be used by helpdesk or service managers to monitor the entire fleet, validate automated actions, and execute them as well, if necessary.

2. **Duration**

   Duration of the Agreement.

3. **Nature and purpose**

   In order to enable the functionalities of the eM services to customers, we store some personal data on the cloud. This is to ensure that the fleet of devices are working and are maintained as expected and to enable Canon to provide support for any customer queries.

   The following elements of the eM service might process personal data:

   (i) The eMaintenance Data Backup Service Option (DBS), which is a service application that periodically makes backups of the setting values (such as the address book and settings/registration) and information of installed MEAP applications that are saved on the hard disk drive of the device. A replaced Hard Drive can have data restored from the cloud speeding up device recovery and its usability. DBS will be storing data from devices which may include, but is not limited to: Address Book information, Server Information, File share information, certificate information, MEAP information. A Device Activation Key is generated by the service provider to activate DBS on eM registered devices. After activation a manual back up or weekly schedule can be used. Data stored in the backup service is encrypted.

   (ii) The eMaintenance Installation Support Service (ISS), which is a cloud service that increases the efficiency of system installation. The service enables automation of the device firmware, additional software installation and device settings by creating an installation model of the target device using the ISS Portal of the service provider. This service also features the option to obtain the information from a DBS profile as agreed with the customer.

   (iii) The eMaintenance common management service, which is utilised across all eM services and provides functions to manage tenants, user accounts, devices, etc. The customer provided administrator account (name and email) can be stored in the management service.

4. **Data categories**

   Name, Email, Telephone and Address, where applicable.

5. **Data subjects**

Any data subject Customer includes in the device address book.

6. Retention Periods

Customer controls the data backup schedule. Data is removed following the termination or expiry of the Agreement.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL SECURITY MATTERS

The below outlines Canon's technical and organisational measures, which Canon may change at any time, so long as it maintains a comparable or better level of security to the measures listed hereunder.

Please note, as eMaintenance is a SaaS offering hosted within the Amazon Web Services data centres, Amazon's security, technical and organisational measures are also relevant and applicable.

Technical Measures

1. **Physical Access Control**

   Canon protects its assets and facilities by only allowing authorized persons to physically access premises, buildings, or rooms where Personal Data is stored.

2. **System Access Control**

   Systems processing Personal Data can only be accessed with authorization. Canon protects its systems and controls access using the following measures:

   - Authorization to critical systems or sensitive information is strictly maintained in accordance with Canon's security policies.
   - All personnel access systems with a unique identifier (user ID) which must not be shared.
   - User roles/permissions are defined, and personnel only have access to the systems that they require to access to fulfil their duties.
   - In case personnel change their assigned role or leave Canon, their access rights are timely adapted or revoked.
   - Canon has an established password policy and each computer locks after a period of inactivity.
   - Canon's network is protected from the public network by firewalls.
   - Canon uses up–to-date enterprise antivirus software.

3. **Data Access Control**

   Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage. Data access is controlled using the following measures:

   - As part of Canon's Security Policy, Personal Data requires at least the same protection level as "confidential" information.
   - Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require to fulfil their duty.
   - Security measures that protect applications processing Personal Data are regularly checked. To this end, Canon conducts internal and external security checks and penetration tests on its IT systems.

4. **Data Transmission Controls**

Except as necessary for the provision of services in accordance with the relevant Agreement, Personal Data must not be read, copied, modified, or removed without authorization during transfer:

- Personal Data transferred over Canon internal networks is protected according to Canon's Security Policy. Network segmentation is in place to ensure isolation between low and high security infrastructure.
- When data is transferred between Canon and its customers this is always conducted across secure encryption transport protocols. In any case, the Customer assumes responsibility for any data transfer once it is outside of Canon-controlled systems (e.g. data being transmitted outside the firewall of Canon's Infrastructure).

5. **Data Input Controls**

Canon implements measures which make it possible to retrospectively examine and establish whether and by whom Personal Data has been entered, modified, or removed from Canon's data processing systems:

- Canon has implemented a logging system for input, modification, deletion, or blocking of Personal Data by Canon or its Sub processors within Canon controlled services to the extent technically possible.
- Canon only allows authorized personnel to access Personal Data as required in the course of their duties.

6. **Job Control**

Personal Data is being processed in accordance with the Agreement and related instructions of the Customer as follows:

- Canon uses controls and processes to monitor compliance with contracts entered between Canon and its customers, sub-processors or other service providers respectively.
- All Canon employees and contractual sub-processors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Canon customers and partners.

7. **Availability Control**

Availability control is provided by AWS and Canon Inc. in accordance with their areas of responsibility.

8. **Data Separation Control**

Personal Data is processed using the following separation controls:

- Canon uses appropriate technical controls to achieve Customer data logical separation.
- Customer (including its approved Controllers) will have access only to their own data based on secure authentication and authorisation.
- Where applicable, a multi-layer tree structure ensures a parent's tenant has access to their children's tenant, however children cannot access other tenants at the same level or at a higher level (such as that of the parents)

9. Data Integrity Control

Personal Data will remain intact, complete and up to date, Canon has implemented a multi-layered defence strategy as a protection against unauthorized modifications.

Organisational Measures

1. POLICIES

Canon's Privacy Accountability Framework consists of a series of policy statements reflecting different aspects of data protection and privacy compliance.

2. GOVERNANCE

A comprehensive governance structure consisting of a network of DPOs and Privacy Champions, with clearly defined roles and responsibilities, is utilised to implement the Accountability Framework throughout EMEA.

3. RISK MANAGEMENT

A number of risk management approaches are utilised to mitigate risks to Personal Data including Privacy Impact Assessments, Data Protection Impact Assessments, Technical and Organisational Measures questionnaires, and comprehensive Vendor Due Diligence procedures

4. CONFIDENTIALITY

Access to customer data is authorised only to the extent necessary to serve the applicable data processing purposes, and all staff with access to customer data are subject to confidentiality obligations.

5. EDUCATION AND AWARENESS

Education and awareness reinforce the Accountability Framework and all staff with access to, or responsibilities for, processing personal data are required to complete appropriate training through Canon's Development Hub.

6. VENDOR DUE DILIGENCE

Third Party companies undergo due diligence assessments and only process customer data in accordance with contractual arrangements.

7. CUSTODIANSHIP

Canon is committed to the safe handling of personal data that we process on behalf of our customers, and we work closely with our partners to help ensure that privacy regulations are complied with.

8. TRANSFER OF DATA

Canon does not transfer data outside a particular jurisdiction without appropriate safeguards, for example Standard Contractual Clauses in the case of the EEA.

9. NOTICE AND TRANSPARENCY

Canon's Privacy notices reflect how the Group manages personal data. Transparency and trust are central principles when processing personal data.

10. PRIVACY BY DESIGN

Privacy is embedded in all products, solutions and services throughout the data lifecycle.

11. CODE OF CONDUCT

Canon adheres to Group Code of Conduct which states that the executive and employees of the Group shall strictly manage all forms of personal information and comply with all applicable laws and regulations and prescribed company procedures.

12. **ACCOUNTABILITY**

Canon demonstrates accountability by maintaining comprehensive internal records of all personal data processing activities, information rights requests, data breaches and risk assessment processes. We also support our customers with their own accountability obligations.

13. INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

Canon has processes to identify, report, manage, recover from, and resolve personal data breaches.

SCHEDULE 3

APPROVED SUB-PROCESSORS

Sub-Processor Name	Address	Location	Purpose
Canon Europa N.V. (Canon)	Bovenkerkerweg 59, 1185 XB Amstelveen, the Netherlands	The Netherlands	Reseller of eMaintenance Suite to Canon
Canon INC	30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo 146-8501, Japan	Japan	Provider of eMaintenance Support services (troubleshooting and maintenance)
Amazon Web Services (JAPAN G.K.)	3-1-1, KAMIOSAKI MEGURO CENTRAL SQUARE SHINAGAWA-KU, TOKYO, 141-0021	Germany	eMaintainance Services digital platform provider