RICOH CloudStream Data Processing Agreement

*Non-English translations of the following content are provided for convenience only. In the event of any ambiguity or conflict between English and the translations, the English version shall prevail.
For a German translation of this document, please check the URL (https://supportsite.eu.cloudstream.ricoh.com/agreement-documents/).

INTRODUCTION
This RICOH CloudStream Data Processing Agreement ("**DPA**") is incorporated into the CloudStream Agreement (the "**Agreement**") and forms a part of the Agreement between Customer and Provider within the meaning of the Agreement (the Provider and the Customer together the "**Parties**"). This DPA governs the processing of personal data by Ricoh or its licensors in the course of providing CloudStream under the Agreement.

AGREED TERMS

1 Definitions
Capitalized terms used in the DPA have the meanings as set forth below. Where a capitalized term is not defined herein, it has the meaning ascribed in the Agreement.

"**Business Day**": Means any day of the week that is not (a) a Saturday, Sunday or a national public holiday in Japan, whereby compensatory holidays that are declared because a national public holiday falls on a Sunday also qualify as national public holidays, or (b) summer holidays or year-end and new-year holidays of the Provider.

"**CCPA**": Means the California Consumer Privacy Act.

"**CPRA**": Means the California Privacy Rights Act.

"**Data Protection Regulations**": Means all laws applicable to any personal data processed under with this DPA, including:

- the Privacy and Electronic Communications Directive 2002/58/EC;
- the EU GDPR;
- the UK GDPR
- the UK Data Protection Act 2018;
- the CCPA;
- the CPRA;
- the laws pertaining to data privacy as enacted by governments of the states and commonwealths in the United States of America;
- all (other) national legislation implementing or supplementing any of the foregoing; and
- guidance issued by any supervisory authority that is binding on the Provider;

all as amended, re-enacted and/or replaced and in force from time to time;

"**EU GDPR**": Means the General Data Protection Regulation (EU) 2016/679;

"**UK GDPR**": Has the meaning given in the UK Data Protection Act 2018;

"**GDPR**": Means the UK GDPR or the EU GDPR, as the context requires;

"**Safe Third Country**": Means country for which the UK Information Commissioner's Office or the EU Commission (as the case may be) has adopted a valid and applicable adequacy decision within the meaning of Art. 45 GDPR.

Other capitalized terms mean the same as used in the Agreement.

2 Terms from the Data Protection Legislation
When used in this DPA, the following terms shall have the same meaning as in the Data Protection Regulations: "**personal data**" (which, if the Customer is subject to the CCPA and/or the CPRA, shall also have the meaning

of “personal information” under the CCPA and/or the CPRA), “**data subject**" (which, if the Customer is subject to the CCPA and/or the CPRA, shall also have the meaning of “consumer” under the CCPA and/or the CPRA), “(**data**) **controller**”, “(**data**) **processor**”, “**processing**”; and “**supervisory authority**”.

3 Background

Under the Agreement, the Provider will provide CloudStream to the Customer either as a cloud service or as software that is licensed to Customer for use as an on-premises application. This involves the processing of personal data by the Provider on behalf of the Customer as described in **Annex 1** (Details of Data Processing), in the former case in order to provide the Cloud Services and in the latter case in connection with the provision of (remote) support services, if any.

4 Description of Processing

1. The subject matter of the processing, the duration of the processing, the nature of the processing, the purpose of the processing, the types of personal data, and categories of data subjects are set out in the **Annex 1** (Details of Data Processing) below.
2. The obligations and rights of the data controller in relation to the processing are set out below together with those of the processor.
3. The Customer discloses the personal data to the Provider only for the limited and specified purposes referred to in this DPA, in particular its Section 6 and its **Annex 1** (Details of Data Processing).

5 Compliance with Data Protection Regulations

The Provider and the Customer shall comply with, and shall ensure that their respective staff and/or subcontractors involved in the processing of personal data comply with, the Data Protection Regulations applicable to them and the DPA.

6 Relationship of the Parties

In relation to the processing of personal data under this DPA as described in **Annex 1** (Details of Data Processing), the Parties acknowledge and agree that:

(a) the Customer is the data controller; and
(b) the Provider is the data processor;

in relation to the processing. If the CCPA applies, then Customer is a *business* and Ricoh is a *service provider* as the CCPA defines those terms.

7 Responsible Individuals and Inquiries

The Customer and the Provider will each notify the other of the individual within its organisation, including subsidiaries, authorised to respond to inquiries regarding the processing of personal data which is the subject of this DPA.

8 Processing of Personal Data by the Provider

In relation to the processing of personal data under this DPA, the Provider shall:

(a) process the personal data, including when making an international transfer of the personal data, only in accordance with the terms of this DPA and on the Customer’s documented instructions unless otherwise required by UK, EU or EU member state law or the law of a Safe Third Country, in which case the processor shall inform the data controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
(b) implement technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing under this DPA, in particular protection against (i) anticipated threats or hazards to the security, confidentiality, and integrity of personal data; and (ii) accidental, unauthorized, or unlawful destruction, loss, alteration, use, disclosure of, or access to personal data transmitted, stored, or otherwise processed under this DPA;
(c) implement restrictions so that only authorised personnel have access to the personal data and that any persons whom it authorises to have access to the personal data processed under this DPA are subject to an obligation of confidentiality in relation to that personal data, such as by means of an appropriate contractual duty of confidentiality and a duty of confidentiality under applicable law;
(d) not engage any sub-processors for the processing of personal data under this DPA unless in accordance with clause 9 of this DPA;
(e) immediately notify the Customer if, in the Provider's opinion, any instruction given to the Provider infringes applicable Data Protection Regulations;
(f) in case the Customer is subject to the GDPR in relation to the processing of personal data under this DPA, assist the Customer in complying with:

(i) the Customer's obligations to respond to requests from any data subject seeking to exercise their rights under Chapter III of the GDPR, taking into account the nature of the processing; such assistance at least including the notification of processor of any data subject request to exercise their rights under Chapter III of the GDPR in due course; and
(ii) the Customer's obligations under Articles 32-36 of the GDPR, taking into account the nature of the processing and the information available to the Provider.

(g) in case the Customer is subject to the CCPA and/or CPRA in relation to the processing of personal data under this DPA,
(i) comply with the applicable obligations under the CCPA and/or CPRA and provide the same level of privacy protection as is required thereunder,
(ii) support the Customer and cooperate with him in taking reasonable and appropriate steps to help ensure that the personal data is used in compliance with this DPA, the CCPA and/or the CPRA, in particular by allowing for monitoring as set out under Section 10 of this DPA;
(iii) notify the Customer if it makes a determination that it can no longer meet its obligations under this DPA, the CCPA and/or the CPRA;
(iv) support the Customer and cooperate with him in taking reasonable and appropriate steps to stop and remediate unauthorised use of personal data;
(v) not sell or share as those terms are defined in the CCPA and/or CPRA the personal data received from the Customer under this DPA;
(vi) not retain, use or disclose the personal data received from the Customer under this DPA for any other purpose other than the business purposes, as those term is defined in the CCPA and/or CPRA, specified in the Agreement and this DPA;
(vii) not retain, use or disclose the personal data received from the Customer under this DPA outside of the direct business relationship between the Customer and the Provider;
(iii) not combine the personal data received from the Customer under this DPA with personal data that the Customer receives from, or on behalf of, any other person, or collects from its own interaction with the data subject, other than allowed for under the CCPA and/or CPRA.

(h) in case the Customer is subject to Swiss data protection law in relation to the processing of personal data under this DPA, comply with the Standard Contractual Clauses – Module 2 as included in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 which is hereby incorporated into this DPA as binding on both parties with the following modifications:
(i) the Customer is the data exporter and the Provider is the data importer;
(ii) Annex I.B. and Annex III will be populated with the information included in **Annex 1** (Details of Data Processing);
(iii) Annex II will be populated with **Annex 2** (Technical and Organisational Measures);
(iv) Clause 7 is included;
(v) Option 2 is chosen for Clause 9(a), and the time period is specified to be ten Business Days;
(vi) the optional part of Clause 11(a) is excluded;
(vii) references to the GDPR are replaced with respective references to the Swiss Data Protection Act;
(viii) references to "EU", "EU Member State", "Member State", "European Union" and "Union" are replaced with references to Switzerland;
(ix) references to the "competent supervisory authority" shall refer to the Swiss Federal Data Protection and Information Commissioner;
(x) governing law for claims under Clause 17 shall be Swiss law;
(xi) Swiss courts shall be chosen for Clause 18(b);
(xii) the term "EU Member State" must not be understood to exclude data subjects from their right to sue for their rights at their place of habitual residence in Switzerland.

9 Sub-processors

1. The Provider shall ensure that any sub-processor it engages to process personal data on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially equivalent to those imposed on the Provider in this DPA or such other alternative terms regarding the processing of personal data on the Customer`s behalf as may be agreed with the Customer (the "**Relevant Terms**"). The Provider shall be directly liable to the Customer for any breach by the sub-processor of any of the Relevant Terms.
2. By entering into this DPA, the Customer approves the engagement of the sub-processors detailed in **Annex 1** (Details of Data Processing). This authorisation constitutes the Customer's prior written consent to the engagement of these sub-processors by the Provider subject to compliance with the requirements set out in Section 9(1) of this DPA.

3. Notwithstanding the above, the Provider is entitled to replace or utilize new sub-processors if the Provider has given the Customer notice of the intention to do so at least ten (10) Business Days prior to such engagement or, as the case may be, replacement, and the Customer has not objected in documented form, subject to compliance with the requirements set out in Section 9(1) of this DPA.

10 Monitoring

The Customer is entitled to monitor and audit the Provider`s compliance with the obligations on commissioned data processing under the applicable Data Protection Regulations and its obligations in relation to data processing under this DPA at any time during normal business hours, generally not more often than once per year unless (i) a data breach has occurred at the Provider, (ii) there are documented facts objectively indicating a violation of Data Protection Regulations or this DPA by the Provider, or (iii) a supervisory authority requests an audit. If the Customer intends to carry out an audit, the Customer shall give the Provider reasonable advance notice of generally at least one month, unless (i) a data breach has occurred at the Provider, (ii) there are documented facts objectively indicating a violation of Data Protection Regulations or this DPA by the Provider, or (iii) a supervisory authority requests an earlier audit, in which case Customer and Provider shall agree on a date that is reasonable and in any case in compliance with Data Protection Regulations. The Provider shall make available to the Customer all information that is necessary to demonstrate compliance with the obligations mentioned in this Section 10.

11 International Transfers

1. The Customer approves the transfer of personal data on behalf of the Customer under this DPA:
   (a) to a third country; or
   (b) to any third party (which shall include any affiliates of the Provider) where such third party is located in a third country.
2. This authorisation constitutes the Customer's prior written consent, where necessary under the applicable Data Protection Regulations, to transfer to third countries as set out in **Annex 1** (Details of Data Processing).

12 Completion of Services

After the end of the provision of CloudStream under the Agreement, the Provider shall delete all personal data (including copies) processed under this DPA, except to the extent that the Provider is required by UK, EU or EU member state law or the law of a Safe Third Country to retain personal data.

13 Requests from Law Enforcement and Regulators

1. If Provider receives a request or demand for Customer's personal data from a law enforcement agency, legislative body, regulator, other governmental entity, or civil litigant (for example, through a subpoena or court order), Provider will attempt to redirect the requestor to Customer. As part of this effort, Provider may provide Customer's contact information to the requestor. If compelled to disclose Customer's personal data by law, Provider will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Provider determines that it is legally prohibited from doing so.
2. To the extent that Customer is unable to independently access the relevant Customer personal data within CloudStream and provided that Customer has configured CloudStream in accordance with Provider's recommendations, then Provider will provide reasonable cooperation to assist Customer to respond to any requests from applicable data protection authorities relating to the processing of personal data under this DPA. In the event that any such request is made directly to Provider, Provider will notify Customer of the request and not respond further to such communication directly without Customer's prior authorization unless legally compelled to do so. If Provider is required to respond to such a request, Provider will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

Annex 1 – Details of Data Processing

Data Subject Categories	Customer will determine the categories of data subjects whose personal data is processed under the DPA. This may include: **For Cloud Services:** • Users of the Cloud Services determined by the Customer • Other natural persons whose personal data may be included in file names **For On-premise solution (including, for the purposes of this DPA, the installation of the Software on the Customer`s private cloud):** • Users and administrators of the Software determined by the Customer • Other natural persons whose personal data may be included in file names
Personal Data Categories	Customer will determine the types of personal data processed under the DPA. This may include: • contact information (such as email address, name, phone number, user id, auth profile, user counter, passwords, department) • information included in file names • location information • IP address • log data (such as access log, audit log, transaction log) • device log files • device data • usage data (such as frequency, timing, duration of access to CloudStream, job history) • preferences (such as frequency of notifications and alerts)
Purposes of Processing (as a processor, for other purposes see Section 6 of this DPA)	**Cloud Services:** To provide the full functionality of CloudStream, including: • To authenticate individual user accounts • To allow functions of CloudStream to work • To communicate with users to address issues and/or queries • To tailor the Customer's and the Customer`s users` experience based on the CloudStream usage by users **On-premise solution:** To provide support services related to the Customer`s use of CloudStream.
Subject-matter/nature of the processing	**Cloud Services:** • When providing CloudStream as a cloud-hosted software-as-a-service, the Customer designates users who receive access to the Cloud Services via individual user accounts. Consequently, account and usage data associated with such accounts is transferred to the servers on which CloudStream is hosted and processed there for the purposes mentioned above. **On-premise solution:** • When providing CloudStream as an on-premise solution, the Customer receives a software license to be installed on the Customer`s own systems. However, in the context of providing support for the use of the Software, the Provider may receive access to the Customer`s systems as well as to account and usage data associated with users and administrators of the Software in order to be able to provide support services.

Sub-processors	To provide CloudStream, the Provider utilises the following sub-processors: **Cloud Services:** • Hosting of CloudStream (Print/Scan function): Amazon Web Services Japan G.K., 3 Chome-1-1, Kamiosaki, Shinagawa City, Tokyo 141-0021, Japan; data centre locations are chosen depending on the location of the Customer: Frankfurt for customers in the EMEA region, London for customers in UK, North Virginia for customers in the US and South America, Montreal for customers in Canada, Australia or Singapore for customers in the Asia-Pacific region. • Hosting of CloudStream (Device Management/Dashboard function): Microsoft Japan, Shinagawa Grand Central Tower, 2-16-3, Konan, Minato city, Tokyo 108-0075 Japan; data centre locations are chosen depending on the location of the Customer: Frankfurt, Germany for customers in the EMEA region, Washington, US for customers in the US and South America, Toronto for customers in Canada, Australia for customers in the Asia-Pacific region. • Order processing: FPT Software, Cebu Ground Floor eBloc Tower 3, Geonzon Street, Cebu IT Park, Lahug Cebu City, Philippines. • Development of Print&Scan services: Y Soft Corporation, Technická 2948/13, Královo Pole, 616 00 Brno, Czech Republic. • Activity, e.g. Providing IT support: affiliates and/or subsidiaries of the Provider as listed in this link [https://www.ricoh.com/about/facts/sales-offices] as of the date of this DPA and as may be updated in accordance with Section 9(3) of this DPA. **On-premise solution:** • Order processing: FPT Software, Cebu Ground Floor eBloc Tower 3, Geonzon Street, Cebu IT Park, Lahug Cebu City, Philippines • Development of Print&Scan services: Y Soft Corporation, Technická 2948/13, Královo Pole, 616 00 Brno, Czech Republic. • Activity, e.g. Providing IT support: affiliates and/or subsidiaries of the Provider as listed in this link [https://www.ricoh.com/about/facts/sales-offices] as of the date of this DPA and as may be updated in accordance with Section 9(3) of this DPA.
Duration of Processing	Personal data may be processed under this DPA throughout the period during which the Provider performs its obligations under the Agreement.
Contact information	ricoh_cloudstream_support_site_admin@jp.ricoh.com

Annex 2 – Technical and Organisational Measures

This Annex 2 outlines the technical and organizational data security measures implemented by the (data) processor to ensure the security, confidentiality, integrity, and availability of the personal data processed on behalf of the (data) controller.
It should be noted that some measures are taken by the (data) processor`s sub-processor(s) on whose processing equipment the data is physically located.

1. Access control
Appropriate measures to ensure that personal data is accessible only by authorized personnel and that access is granted based on the principle of least privilege.
(a) Physical access control (so-called entry control)
Appropriate measures to prevent unauthorised access to data processing facilities:

- With regard to the facilities of the sub-processor that operates the data processing facilities on which the data is physically located, these measures are set out in the public documents below:
  •Azure
  https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
  •AWS
  https://aws.amazon.com/compliance/data-center/controls/
- The Processor does not physically access the sub-processor's physical server. The links above shall apply when the Processor accesses such server remotely.

(b) Electronic access control
Appropriate measures to prevent unauthorised use of the data processing systems:

- *passwords and security rules for passwords (minimum password length, character type requirements) for customer administrator accounts*
- *encryption of data at rest*
- *authorisation concept*
- *access logs*
- *firewalls*

2. Transfer control
Appropriate measures to prevent unauthorised reading, copying, changing or deleting of personal data during or as a result of electronic transfer or transport:

- *encryption of data in transit*

3. Isolation control
Appropriate measures to ensure the separation of personal data processed on behalf of separate controllers:

- *multiple client support*
- *logical separation of clients*

4. Availability and resilience
Appropriate measures to ensure the protection of personal data against loss, corruption or destruction:

- *regular backups (across different and redundant servers)*
- *malware protection*
- *redundancy*

5. Testing, assessment and evaluation

- *Appropriate vulnerability assessments to ensure compliance with and effectiveness of data security measures:*
- *Data protection management system (such as security training)*
- *Regular and incident-based sub-processor oversight*
- *Regular security assessments*