Konica Minolta Workplace Pure Data Processing Agreement

according to Art. 28 GDPR

between

Customer

(insert company name, address, postcode, city, country)

as Controller according to GDPR

and

Konica Minolta Business Solutions Europe GmbH

Europaallee 17, 30855 Langenhagen, Germany

as Processor according to GDPR

together “the Parties”

§ 1 Purpose of the Agreement

(1) The Processor provides the Konica Minolta Workplace Pure cloud service provisioning and management platform to the Controller subject to the terms agreed in the Workplace Pure terms and conditions – hereinafter referred to as the "Principal Agreement". Providing and maintaining the Workplace Pure cloud service provisioning and management platform involves processing of personal data by the Processor on behalf of the Controller. To define their respective rights and duties regarding the processing of personal data on behalf of the Controller the Parties conclude this data processing agreement ("DPA").

(2) The personal data processed under the DPA may be data originating from the Controller or processors associated with the Controller under Art. 26 or 28 GDPR, or data collected by the Processor for the aforementioned (all such data hereinafter jointly referred to as "Controller's personal data"). The specific type of Controller's personal data processed by the Processor, the categories of data subjects concerned by the processing and the nature and purpose of the processing are further specified in Annex I to this DPA.

(3) The duration of the data processing and the term of this DPA shall be based on the term agreed in the Principal Agreement or shall continue for as long as required by applicable statutory provisions. Further obligations or exceptional rights of termination may arise from further provisions of the Principal Agreement or this DPA.

§ 2 Right to Issue Instructions

(1) The Processor may only collect, process, or use data within the scope of the Principal Agreement and in accordance with the instructions of the Controller.

(2) The instructions of the Controller are initially set out in this DPA and may subsequently be amended, supplemented, or replaced by individual instructions in writing or in text (individual instructions). Verbal instructions are confirmed by the Controller without delay (at least in text form). The Controller is entitled to issue instructions at any time. This includes instructions regarding the erasure, rectification, and restriction of processing of data. For services for the use of which this is required, persons authorised to give and receive instructions are defined in Annex I.

(3) If the Processor is of the opinion that an instruction of the Controller violates data protection regulations, the Controller must be informed immediately. The Processor shall be entitled to suspend the execution of the instruction in question until it is

confirmed or amended by the Controller. The Processor may refuse to carry out an instruction which is manifestly unlawful.

(4) Instructions of the Controller which go beyond the services owed under the Principal Agreement and the data processing required for this and which the Processor is not legally obliged to provide could be subject to separate remuneration.

§ 3 Security Measures of the Processor

(1) The Processor is committed to comply with the provisions of law on data protection. Within its area of responsibility, the Processor shall design the organisation in such a way that it meets the special requirements of data protection. The Processor shall take all necessary technical and organisational measures for the appropriate protection of the personal data of the Controller in accordance with Art. 32 GDPR, in particular at least the measures listed in Annex I. The Processor reserves the right to modify the security measures taken, while ensuring that they do not fall below the contractually agreed level of protection.

(2) The Processor shall appoint a company data protection officer. The contact details of the data protection officer shall be published on the Processor's website and communicated to the competent data protection supervisory authority.

(3) Persons employed by the Processor in the processing of data on behalf of the Controller shall be prohibited from collecting, processing, or using personal data without authorisation. The Processor shall impose an obligation of confidentiality (Art. 28 (3) lit. b GDPR) on all own personnel entrusted with the processing and fulfilment of this DPA (hereinafter referred to as employees) and shall ensure compliance with this obligation with due care. The obligation of confidentiality must be formulated in such a way that it remains in force even after the termination of either this DPA or the employment relationship between the employee and the Processor.

§ 4 Duties of the Processor

(1) In the event of a personal data breach of personal data of the Controller, the Processor shall immediately inform the Controller in writing or text form. The notification of a personal data breach shall at least contain a description of:

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

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained,

(c) the likely consequences of the personal data breach,

(d) 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.

(2) The Processor shall immediately take the necessary measures to secure the personal data and to mitigate any adverse consequences for the data subjects, shall inform the Controller thereof, and request further instructions.

(3) In addition, the Processor shall be obliged to provide information to the Controller at any time in so far as personal data are affected by a breach as referred to in paragraph (1).

(4) If the personal data of the data Controller at the Processor's premises are endangered by attachment or confiscation, through insolvency or settlement proceedings or through other events or measures of third parties, the Processor shall inform the Controller immediately, unless this is prohibited by court or official order. In this context, the Processor will without delay inform all jurisdictional authorities that the power of ultimate decision over the data lies exclusively with the Controller in its capacity as "Controller" within the meaning of the GDPR.

(5) The Processor shall keep a record of processing activities carried out on behalf of the Controller, containing all the information required by Art. 30 (2) GDPR.

(6) The Controller and the Processor will if requested to do so assist the data protection supervisory authorities in the fulfilment of their duties.

§ 5 Rights of the Controller

(1) The Controller will prior to the commencement of data processing, and regularly thereafter, establish to their satisfaction the adequacy of the technical and organisational measures taken by the Processor. For this purpose, the Controller may, for example, obtain information from the Processor, have existing certifications or attestations from experts presented to them or, after timely coordination (at least three weeks in advance), inspect the technical and organisational measures of the Processor. Inspections may be performed during normal business hours personally or by a competent third party. Inspections by third parties must be performed in agreement with the Processor, third parties in a competitive relationship may be rejected by the Processor. The Controller shall carry out inspections only to the extent necessary and shall not disrupt the

operations of the Processor disproportionately. Each party shall bear its own costs for audits and inspections.

(2) The Processor undertakes to provide the Controller, at the latter's written request and within a reasonable period of time, with all the information necessary to carry out an audit or inspection on the technical and organisational measures taken by the Processor.

(3) The Controller shall document the result of the audit or inspection and provide it to the Processor. In the event of errors or irregularities which the Controller discovers, in particular in the results of commissioned data processing, the Processor shall be informed without delay. If the audit or inspection reveals issues the future avoidance of which requires changes to the commissioned processing, the Controller shall inform the Processor of the findings and requested changes in writing or in text form.

(4) The Controller bears responsibility for assessing the lawfulness of the data processing.

§ 6 Engagement of Sub-Processors

(1) The services agreed in the Principal Agreement or partial services thereof will be carried out with the involvement of the Sub-Processors (subcontractors) listed in Annex I. Within the scope of its contractual obligations, the Processor shall be authorised to modify existing subcontractor relationships or to establish new ones. The Processor shall immediately inform the Controller thereof. The Controller may object to the engagement of new subcontractors. The Controller must raise any objection immediately; objections may not be based on extraneous considerations.

(2) The Processor is obliged to carefully select subcontractors according to their suitability and reliability. If subcontractors are used, the Processor shall engage them in accordance with the provisions of this DPA. If subcontractors in a third country are to be involved, the Processor shall ensure that an appropriate level of data protection is guaranteed for the respective subcontractor (e.g. by agreeing on the EU standard contractual clauses).

(3) A subcontracting relationship within the meaning of these provisions shall not exist if the Processor commissions third parties with services which are to be regarded as purely ancillary services. These include, for example, postal, transport and dispatch services, cleaning services, telecommunications services without any specific reference to services which the Processor provides for the Controller, and security services.

§ 7 Queries and Rights of Data Subjects

(1) Where possible, the Processor shall support the Controller with suitable technical and organisational measures to help fulfil the Controller's obligations under Articles 12 to 22 and 32 to 36 GDPR.

(2) If a data subject should contact the Processor directly in order to assert their rights as data subject, for example to obtain information, rectification or erasure of their data, the Processor will not react independently. If the responsible Controller can be identified from the data subject request, the Processor shall inform the Controller and await the latter's instructions.

§ 8 Liability

(1) The Controller assumes complete responsibility for any claims brought against the Processor by reason of any loss or damage suffered by a data subject as a result of data processing or the use of data in the course of processing that is prohibited or incorrect pursuant to data protection regulations insofar as the prohibited or incorrect data processing or use of data is based on instructions issued by the Controller.

(2) Each of the Parties will release the respective other Party from liability if that other Party can prove that it was in no way responsible for the circumstance leading to the loss or damage suffered by the data subject.

§ 9 Termination of the Principal Agreement

(1) After termination of the Principal Agreement or at any time at the request of the responsible party, the Processor shall return to the responsible party all documents, data and data carriers provided by the Controller or – at the request of the Controller, unless there is an obligation to store personal data under applicable law – erase them.

(2) The Processor shall be obliged to treat confidentially the data that has become known to them in connection with the Principal Agreement during and beyond the end of the term of the Principal Agreement. This DPA shall remain in force beyond the end date set out through the Principal Agreement for as long as the Processor has Controller's personal data at its disposal.

§ 10 General Provisions

(1) The Parties agree that the Processor waives reliance on the right of retention within the meaning of § 273 of the German Civil Code (Bürgerliches Gesetzbuch – BGB) in respect of the data to be processed and related electronic media.

(2) Changes and amendments to this DPA must be made in writing. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements remains unaffected.

(3) In case of doubt, the provisions of this DPA take precedence over the provisions of the Principal Agreement.

(4) Should individual provisions of this DPA be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions.

(5) Place of jurisdiction is Hanover.

Signatures

Date:	Date: 07.07.2022
For the Controller:	For Konica Minolta:
Name:	Name: Tadahiko Sumitani
Position:	Position: President

Date:

For the Controller:

Name:

Position:

(Signature of a second person only if the legal business form of the Controller so requires.)

Annex I to the Konica Minolta Data Processing Agreement

Description of the data processing in

Workplace Pure

Cloud service provisioning and management platform

v2.5 BEU EN – 18-05-2022

1. Description of the nature and purpose of the processing

2. Description of the type of personal data and categories of data subjects

3. Engaged Sub-Processors

4. Technical and organisational measures

5. Persons authorised to issue and receive instructions

1. Description of the nature and purpose of the processing

Konica Minolta is obligated to provide and maintain the Workplace Pure cloud service provisioning and management platform to the Controller in accordance with the Principal Agreement.

Via the Workplace Pure cloud platform, Konica Minolta provides the Controller with a variety of applications and functions for the more efficient handling of customer-specific workflows. Services such as Cloud Print or Document Convert services are made available via the front-end of Workplace Pure. The connection to some services operated by the Controller, such as dropbox, SharePoint, or GoogleDrive is made via dedicated Workplace Pure connectors. The back-end of the Workplace Pure platform allows the Controller to perform evaluations and customer management, and access help desk functions. The Workplace Pure services can be used via various Controller operated end devices: Multifunctional Printers, PC, mobile phones, etc.

When using Workplace Pure, personal data or documents of the Controller or third parties (hereinafter jointly referred to as "Personal Data of the Controller") will be processed by Konica Minolta. However, all Personal Data of the Controller will be

deleted from the cloud service after a processing operation, unless the Controller makes explicit arrangements for continued storage.

With the "Security Cube" feature the processing of data sets within Workplace Pure can be carried out under pseudonymisation of user identifiers (user personal data such as name and email address). Personal user identifiers are then stored and processed separately from the pseudonymised data sets.

The specific nature of processing will depend on the Workplace Pure features used by the Controller. The Controller may change the access to functions at any time.

The Controller will assess the permissibility of any data processing carried out in Workplace Pure. Konica Minolta will not independently process the Personal Data of the Controller.

Further details on the scope and purpose of the processing of the Personal Data of the Controller by Konica Minolta may result from the Principal Agreement or any supplementary agreements.

2.1 Type of personal data

Type of personal data contained in Controller documents:
[The type of personal data depends on the content of the documents processed with Workplace Pure and can only be determined by the Controller.]

☐ Personal master data (e.g. first name and surname)
☐ Communication data (e.g. telephone, email)
☐ Contract master data (e.g. contractual relationship, product/contractual interest)
☐ Customer history (e.g. CRM data)
☐ Contract billing and payment data
☐ Credit card data and bank data (bank account numbers)
☐ Planning and controlling data
☐ Information obtained from third parties (e.g. credit agencies, public directories)
☐ Connection data (e.g. IP addresses, MAC addresses)

☐ Other:

2.2 Categories of data subjects

Categories of data subjects affected by the processing:
[The categories of data subjects affected by the data processing can exclusively be determined by the Controller].

☒ Employees (Art. 88 GDPR)
☐ Customers
☐ Prospective customers
☐ Subscribers
☐ Suppliers
☐ Business contacts
☐ Minors (e.g. apprentices, trainees, interns)

☐ Other:

3. Sub-Processors

First level and local language support will be provided through Konica Minolta Business Solutions National Operating Companies in respective Controller country of location. All such 100% Konica Minolta Europe owned affiliates can be contacted through:

Konica Minolta Business Solutions Europe GmbH
Europaallee 17
30855 Langenhagen
Germany

Description of the commissioned processing for Konica Minolta local affiliates:

- First level and local language support

Description of the commissioned processing for Konica Minolta Europe:

- Operation of IT infrastructure including support ticket management for all Konica Minolta European operations
- 2nd and 3rd Level Support for Workplace Pure cloud platform

Telekom Deutschland GmbH
Landgrabenweg 151

53227 Bonn
Germany

Description of the commissioned processing:

- The Workplace Pure cloud platform is hosted with Telekom Deutschland

alemo Kommunikations GmbH
Alter Wandrahm 8
20457 Hamburg
Germany

Description of the commissioned processing:

- 3rd level support for the Workplace Pure cloud platform

For some **Workplace Pure optional modules or functionalities, additional sub-processors will be employed.** These additional sub-processors are **announced and managed via the Workplace Pure administrative console**. All persons granted Workplace Pure administration rights by the Controller are persons authorised to give instructions within the meaning of Art. 29 GDPR and § 2 (2) of the Konica Minolta DPA.

Should any further addition or replacement of sub-processors become necessary, the information according to Art. 28 (2) GDPR and § 6 (1) of the Konica Minolta DPA will also be provided via the Workplace Pure cloud platform.

4. Technical and organisational measures

1 1. Confidentiality

1.1 1.1 Physical access control

The measures by which unauthorised persons are denied entry to data processing systems used for processing personal data are described below:

- Definition of entry-authorised persons by means of organisational specification
- Documentation of the allocation and retraction of entry rights
- Regular review of entry rights
- Access regulations for external persons
- Documentation of presence in the server rooms
- Access-secured premises with entry for authorised persons only

- Alarm security and video surveillance of premises as well as inside the buildings incl. the server rooms
- Access control depending on the security area either with personalised ID card including photo and access card with PIN code or with personalised token, biometric access control (fingerprint), and separation system or keys

1.2 1.2 System access control

The following measures are taken to prevent the intrusion of unauthorised persons into the data processing systems:

- Use of complex passwords with at least eight characters that fulfil at least three of four criteria (upper case letter, lower case letter, numeral, special character) and a mandatory change of password every 90 days
- Ban on password disclosure
- Separation into administrator and user profiles
- Logging of allocated system access rights
- Limitation of administration access to the minimum
- Automatic locking of systems after defined period out of use
- Logging of access rights changes

1.3 1.3 Data access control

Unauthorised activities in data processing systems outside the scope of allocated rights will be prohibited by means of access rights and an authorisation concept with a needs-based design, and by means of their inspection:

- Limitation of access rights to scope of activity of specific employee
- Separation of access right permission (organisational) and access right allocation (technical)
- Specific access rights corresponding to data/file access requirements
- Logging of allocated data access rights
- Allocated access rights are regularly audited and updated
- Protection of data processing systems against unauthorised access by means of adequate firewall systems
- Logging of unauthorised access attempts

1.4 1.4 Separation control

- Separation of productive and test environments by technical measures (virtual servers, separated systems, IP-address-segmentation)

1.5 1.5 Pseudonymisation

- When transmitting data sets, use is made of the possibilities of pseudonymisation (and anonymisation where possible)
- When transmitting pseudonymised data, it is ensured that the pseudonym cannot be reunited with the data set owner information at the recipient's end

2 2. Integrity

2.1 2.1 Transmission/transfer control

- Encryption of data transfer, particularly when transferring over public networks (e.g. SSL, TLS)
- Data protection-compliant eradication and/or destruction of data, data storage devices and printed copies in accordance with an information classification concept
- Encryption of data storage devices
- Remote-wipe option for mobile devices

2.2 2.2 Input control

- The logging of data processing enables later inspection and determination of whether and by whom personal data has been entered, altered, or removed (e.g. data amendment logs in central ERP systems)
- Recording and needs-based retainment of corresponding actions carried out on systems (e.g. log files)

3 3. Availability and load ability: Control of availability and the ability to restore

- Use of multiple, geo-redundant, certified data centres, which prevent service interruptions by mirroring
- Technical precautions in the form of early warning systems for protection against disruptions caused by fire/heat, water, or overheating
- Measures to protect against loss of power and current overload, e.g. uninterruptible power supply (UPS)

- Scheduled performance of data backups and additional use of mirroring procedures
- Multi-layered antivirus/firewall architecture
- Established process for central procurement of hardware and software
- Regular updates of all systems in use
- Protocols for emergency measures and data recovery in place

4 4. Order control

- Appointment of a data protection officer
- Service-level agreements with and GDPR compliant engagement of external service providers
- Instruction of employees in processing personal data
- Commitment of employees to data secrecy

5 5. Control of organisation (assessment, scoring, and evaluation)

- Continuous processes are established for assessment and if necessary, adjustment of data protection measures
- Processes are established for data breaches and other violations of the confidentiality of personal data
- Data processing by employees only takes place with documented instruction from management or superior
- Mandatory company policies are established on treatment of personal data as well as usage of IT systems
- Corresponding trainings of employees
- Incident-response-management

5. Persons authorised to issue and receive instructions

All persons granted Workplace Pure administration rights by the Controller are persons authorised to give instructions within the meaning of Art. 29 GDPR and § 2 (2) of the Konica Minolta DPA.