



KONICA MINOLTA

Data Processing Agreement

VERSION 8 BBE: 01.04.2024

§ 1 Purpose of the Agreement

- (1) The Processor provides services to the Processor (hereinafter also referred to as "Customer") as governed by the underlying agreement to rent/purchase multifunction copiers with associated maintenance services (hereinafter referred to as the "Principal Agreement"). To the extent that the provision of these services involves the processing of personal data on behalf of the Controller, as referred to in the General Data Protection Regulation which entered into force on 25 May 2018 (hereinafter: GDPR), the Parties hereby lay down their respective rights and obligations in the present data processing agreement (hereinafter: "DPA")
- (2) The processed personal data may be data that originate from the Controller or controllers or processors associated with the Controller under Section 26 or Section 28 of the GDPR, or personal data that were collected by the Processor on behalf of the aforementioned (all personal data will hereinafter jointly be referred to as "Controller's personal data").
- (3) The type of Controller's personal data and categories of personal data subjects affected by the processing as well as the nature and purpose of the processing are specified in annex 1 of this DPA
- (4) The duration of the processing and the term of this DPA shall depend on the term of the Principal Agreement(s) unless for the provisions which impose obligations or rights of termination that go beyond this.

§ 2 Right to Issue Instructions

- (1) The Processor may only collect, process, or use data within the scope of the Principal Agreement(s) 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.



KONICA MINOLTA

This includes instructions regarding the erasure, rectification, and restriction of processing of data. For products whose use requires it, persons authorised to give or receive instructions are defined in the respective annex 1 to this DPA.

- (3) If the Processor is of the opinion that an instruction of the Controller violates data protection regulations, the Controller must be informed as soon as possible. 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(s) and the data processing required for this, could be subject to separate remuneration to the Controller.

§ 3 Security Measures of the Processor

- (1) The Processor is committed to comply with the GDPR. 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 specified in annex1. The Processor reserves the right to modify the security measures taken, while ensuring that they do not fall below the level of protection as agreed in the Annex 1 to this DPA..
- (2) The Processor appointed a company data protection officer. The contact details of the data protection officer are published on the Processor's website .
- (3) 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.

§ 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,



KONICA MINOLTA

- (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



KONICA MINOLTA

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 and evidence 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.

§ 6 Engagement of Sub-Processors

- (1) By signing this Agreement, the Processor receives a general authorization to appoint Subprocessors for the performance of the Principal Agreement. The appointed Subprocessors are listed in annex 1.
- (2) the Processor shall be authorised to modify existing subcontractor relationships or to establish new ones. The Processor shall as soon as possible 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.
- (3) 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).
- (4) 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.



KONICA MINOLTA

§ 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, within the limits of the principal agreement, 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(s)

- (1) After termination of the Principal Agreement(s) 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 or overwrite them. This also applies to any data backups at the Processor's premises. The Processor is entitled to invoice the Controller for a deletion or data overwrite of the personal data stored on the hard drive of a multifunction copier.
- (2) The Processor shall be obliged to treat confidentially the data that has become known to them in connection with the Principal Agreement(s) during and beyond the end of the term of the Principal Agreement(s). This DPA shall remain in force beyond the end of the Principal Agreement(s) for as long as the Processor has personal data at its disposal



KONICA MINOLTA

which have been provided by the Controller or which has been collected by the Processor on the Controller's behalf.

§ 10 General Provisions

- (1) Changes and amendments to this DPA must be made in writing.
- (2) This DPA forms an integral part of the Principal Agreement. All rights and obligations under the Agreement, including limitations of liability, therefore also apply to this DPA. In case of contradiction, inconsistency or doubt between the terms and conditions of this DPA and the terms and conditions of the Principal agreement, the conditions of this Principal Agreement will take precedence over the conditions of the DPA.
- (3) 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.
- (4) This Agreement will be governed by Belgian law and in case of any dispute the court of Brussels or Antwerp, at Processor's discretion, is the competent court.

Annex to the Konica Minolta DPA

Description of the technical and organizational security measures

1. Description of the nature and purpose of the processing during the use of Printing Systems

Konica Minolta Multifunctional and/or Production Printings Systems process paper and electronic documents for the purposes of printing, scanning, copying, and faxing.

The processing of personal data of the Controller or third parties (in the following jointly referred to as "personal data of the Controller") by Konica Minolta is exclusively carried out within the scope of providing service and maintenance to Konica Minolta Systems. The personal data will only be processed with the purpose of performing service and maintenance. Further collection or use of the personal data of the Controller by Konica Minolta does not take place. The specific nature of processing will depend on the service options and remote services described in this Annex that have been chosen by the Controller.



KONICA MINOLTA

The processing of personal data of the Controller might occur in the course of provisioning and setting up Konica Minolta Systems (especially in the context of a network connection) and in the course of physical servicing and maintenance work on the equipment.

Konica Minolta Multifunctional and Production Printing Systems are able to record technical processes in encrypted log files. Konica Minolta does not initiate the creation of log files until error analysis becomes necessary. The log files might be accessed by a Konica Minolta technician on site, however in standard procedure log files are transferred to servers owned and operated by Konica Minolta Europe (server location Germany) as part of the Konica Minolta remote services (Konica Minolta "Remote Service Platform" – "RSP").

Furthermore remote services can be used to create backup copies of the equipment configuration, which can be stored in a password-protected and encrypted form on either Controller's own servers or Konica Minolta Europe servers (server location Germany).

Both log files and backup copies of the device configuration do not contain any contents of print, scan, copy, or similar operations performed on the Systems.

Remote service and maintenance of Konica Minolta Systems will be carried out according to the service options chosen by the Controller. For this purpose Konica Minolta operates the "Konica Minolta Remote Service Platform" (RSP), Remote Panel connections, the solution "Konica Minolta Remote Support Tool", or functionally comparable solutions. When carrying out remote maintenance, it is not possible to completely eliminate the possibility of viewing and thereby processing personal data of the Controller.

In the event of a possible return of Konica Minolta Systems after the end of the term of the Principal Agreement, the personal data on the hard drive of the equipment and in the internal memory will be either destroyed, erased, overwritten or handed over to the Controller.

2.1 Type of personal data during the use of printing systems

General: data of Data Subjects to which Konica Minolta will have access under the Main Agreement with the Customer.



KONICA MINOLTA

Type of personal data that may be included in backup copies of the device configuration: Equipment's internal address book (IT user names and email addresses), IP addresses, MAC addresses, serial number

Categories of personal data possibly contained in log files:

IT user names (e.g. Windows user names of the users of the device), user e-mail addresses, IP addresses, MAC addresses, serial number, history of the device's internet browser (accessed URLs), history of the device power status, print job history of the last 150 print jobs (owner of the print job, time stamp, document name).

All data recorded in log files are only collected starting with initiation of event logging.

Personal data that might be processed during on-site service and maintenance:

[The type of personal data possibly accessible to Konica Minolta technicians depend on the data processed on the Systems. These contents can only be assessed 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) ☒ IP addresses, MAC addresses
- ☐ Other:

2.2 Categories of data subjects

Categories of data subjects affected by the processing:

[The following categories of owners of the personal data listed under 2.1 can only be assessed by the Controller.]

- ☒ Controller employee personal data (under Art. 88 GDPR)
- ☐ Controller's business partner employee data
- ☐ Controller's B2C end-customer data
- ☐ Further business contact data
- ☐ Minors' data (e.g. apprentices or interns within any of the above groups)
- ☐ Other:



KONICA MINOLTA

3. Engaged Sub-Processors

Konica Minolta Business Solutions Europe GmbH

Europaallee 17
30855 Langenhagen
Germany

Description of the commissioned processing:

- IT Service Provider for Konica Minolta Business Solutions Belgium NV (including operation of Konica Minolta remote service and backup servers)
- Hosting of the SafeQ Cloud Print Solution within the KONICA MINOLTA CLOUD, with all data centres owned and operated by Konica Minolta Europe
- 2nd Level Support on the printing systems and Safe Q Cloud solutions for Konica Minolta Business Solutions Belgium NV

YUSEN LOGISTICS (Benelux) BV

Middenweg 10
4782 PM Moerdijk
the Netherlands

Description of the commissioned processing:

- Logistic service provider (delivery and installation of the MFP's, hard disk overwrite and/or erase at the end of the Principal Agreement)

FOUNDEVER Operating Corporation Limited

Butts Road 53-55 Coventry
Warwickshire CV1 3 BH
England

Description of the commissioned processing:

- Call center for every request for maintenance interventions or delivery of supplies from and to customer – Konica Minolta informs Controller of the fact that England as part of the United Kingdom is considered as a country with an adequate level of data protection in accordance to the adequacy decision of the European Commission (art. 45 GDP)

I.S.A.B. NV

Huttegem 10,
8570 Anzegem
Belgium

Description of the commissioned processing:



KONICA MINOLTA

- Maintenance service provider on the MFP devices of some customers

4. Technical and organisational measures

1. Confidentiality

a) Physical access control:

- Only persons who need to see personal data as part of their job title (function) are authorized to process personal data
- It is established which functions these are and this is monitored
- Periodic audits of access control.
- Access control in premises of processor with badge, including server room
- Documentation of presence in server rooms
- Access control for external persons

b) Control of system and data access

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

- Admission to the systems is possible after multi factor authentication with an individual user name and password
- 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
- Logging of access rights allocations
- Limitation of administration access to the minimum
- Protection of data processing systems against unauthorized access by means of appropriate firewall systems
- Automatic locking of systems after defined period out of use
- Allocation of access rights based on an authorisation concept with a needs-based design
- Regular auditing of access rights
- Separation of rights permissions (organisational) from rights allocations (technical)

c) Control of separation :

- Logging of rights amendments Checks on unauthorised access attempts (IDS/IPS) Specification of different user profiles (administrator/user levels)
- Specification of different user profiles (administrator/user levels)
- Specific access rights corresponding to data access requirements
- Separation of productive and test environments by technical measures (virtual servers, separated systems, IP-address-segmentation)

2. Integrity



KONICA MINOLTA

a) Transmission 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 a protection class concept
- Encryption of data storage devices
- Remote-wipe option for mobile devices

b) Input control:

- Access rights are regularly checked and updated
- 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)
- Only for Printing systems: Unique identification and tagging of data storage of MFP/PP-devices for at return

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

- Use of two certified IT centres that are located far apart from each other, thereby preventing service interruption by mirroring (i.e. by retention of redundant data)
- Only for printing systems: Technical precautions in the form of early warning systems for protection against disruptions caused by fire/heat, water or overheating
- Only for printing systems: Measures to protect against loss of power and current overload, e.g. uninterruptible power supply (UPS) systems
- Only for printing systems: 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
- Ability to restore in a timely manner (Art. 32 sec.1 lit. c GDPR) via global system-related backup-concept
- Regular updates of all systems in use, where applicable
- Protocols for emergency measures and data recovery in place

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
- Mandatory compliance of employees with data secrecy



KONICA MINOLTA

- Technical safeguarding through measures for access, separation and input controls

5. Control of organisation (verification, valuation and evaluation):

- Continuous processes for verification and if necessary adjustment of data protection measures are established
- Processes for dealing with a data protection case in place
- company guidelines on treatment of personal data as well as usage of IT systems in place
- Corresponding trainings of employees with regard to it security and GDPR
- Incident-response-management