KONICA MINOLTA

KONICA MINOLTA AND DATA PROTECTION

OUR BUSINESS APPROACH

July 2018

Giving Shape to Ideas

1. INTRODUCTION

Konica Minolta Business Solutions (UK) Limited take the requirements and implications of GDPR very seriously and have been working both locally and at a European level to ensure there are sufficient controls in place to enable compliance.

https://www.konicaminolta.co.uk/business-solutions/company/company-information/global-personal-data-protection.html

As well as taking it seriously at a business level, we also have in place a number of tools that can help customers meet their compliance requirements.

We have appointed a Data Protection Officer, Salman Khan, dataprotection@konicaminolta.co.uk

2. TECHNICAL AND ORGANISATIONAL MEASURES

As a business, Konica Minolta Business Solutions have in place a number of technical and organisational measures that ensure data is kept secure and data subjects have the ability to establish their rights over their data as put in place by the Data Protection Act 2018 and the General Data Protection Regulation.

These are outlined below.

2.1 Confidentiality

2.1.1 Control of physical access

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 auditing of entry rights
- Entry control with personalised photographic ID
- Entry control with personalised token and separation system
- Documentation of presence in the server rooms
- Entry regulations for external persons
- Closed areas with entry for authorised persons only
- Video monitoring of this area and inside the building, including the server rooms

2.1.2 Control of system access

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

- Admission to the systems is possible only after 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 unauthorised access by means of appropriate firewall systems

2.1.3 Control of data access

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 admission rights to areas of activity
- Separation of rights permissions (organisational) from rights allocations (technical)
- Logging of rights amendments
- Checks on unauthorised access attempts (IDS/IPS)

2.1.4 Control of separation

- Specification of different user profiles
- Specific access rights corresponding to data access requirements and role
- Separation of the data from multiple applications by using virtual machines (for individual applications)

2.2 Integrity

2.2.1 Control of transmission

- Encryption of data transfer, particularly when transferring over public networks (e.g. SSL, TLS) and via email
- Data protection compliant eradication of data, data carriers and printed copies in accordance with a protection class concept

2.2.2 Control of input

- Access rights are regularly checked and updated
- Logging of data processing (where possible and applicable) to enable 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 availability of corresponding actions carried out on systems (e.g. log files)
- Explicit identification and tagging of data storage of MFP/PP-devices for return

2.3 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)
- 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) systems
- Scheduled performance of data backups and, if necessary, use of mirroring procedures
- Multi-layered antivirus/firewall architecture
- Central procurement of hardware and software
- Ability to restore in a timely manner (Art. 32 sec. 1 lit. c GDPR)

2.4 Control of orders

- Appointment of a Data Protection Officer
- Service-level agreements with external service providers
- Training and instruction provided to Colleagues about processing personal data
- Mandatory compliance of Colleagues with data secrecy

2.5 Control of organisation (verification, valuation and evaluation)

- Continuous processes established for verification and adjustment of data protection measures if required
- Regulation set out in writing for data copies
- Processes established for dealing with data protection enquires (e.g. SAR, deletion etc.)
- For each relevant process a risk assessment has been completed
- For each relevant process an impact assessment has been completed
- Data protection-friendly basic settings are implemented
- Incident-response-management process and responsibilities in place

3. MACHINE SECURITY

All machines have in place a hard drive but this is not only secure storage but a form of 'holding pen' for the data to be printed. Once the job has been released and printed, or after a set period of time if not released (usually 24/48 hours depending on initial set up) it is no longer held on the drive. Further information about this can be found on our security pages here: https://www.konicaminolta.co.uk/business-solutions/products/security.html

4. PROCESSING METHODS

Below are the answers to some common questions about how we process any personal data we may hold on you.

What data are we processing?	Contact details (name, address, email, phone number). Any user data required to set up the machines in place or attend to any queries or service requests.
Where is data hosted?	In Germany by our parent company and in the UK.
How long is data retained for?	Data is held for the duration of the contract between the customer and Konica Minolta and for any required legal reporting e.g. financial reporting – up to seven years

Does any sub-processing take place?	Sub-processing occurs in relation to: • Details provided to our support desk provider (Romania) • Details provided to our logistics providers to deliver and collect equipment (UK) • Details provided to our consumable recycling provider to enable collections (UK) • (If relevant) details provided to any leasing company for the leasing of equipment (various companies, UK)
Who has access to the data?	Access to data is provided on a role basis to ensure those providing billing and service support have access to the data required to provide contracted services
Who is accountable for the data?	All Colleagues are accountable for the data they use and have access to, but ultimately the responsibility sits with the Data Protection Officer
In the event of a data breach, what is the process?	Any data breach is reported according to our Incident, Accident and Near Miss Reporting procedure and categorised and managed accordingly.
How will you notify us if a breach occurs?	Any breach will be notified in writing, likely via email, with details of the breach, what action has been taken, what actions are planned and who the responsible officer is.