Die nächsten Seiten enthalten den unterzeichneten **Auftragsverarbeitungs-Vertrag** für Service und Wartung von Multifunktions-Systemen (MFP) & Production Printing-Systemen.

Bitte folgen Sie den nachstehenden Anweisungen zum Ausfüllen, Unterzeichnen und Übersenden des Dokuments an Konica Minolta:

Schritt 1: Lesen Sie das Dokument sorgfältig durch und füllen Sie die grün und gelb markierten Felder aus. Diese Felder enthalten Informationen über den Namen und die Adresse Ihres Unternehmens sowie über die Art der personenbezogenen Daten, die Ihr Unternehmen über unsere Systeme verarbeiten wird. Füllen Sie die kurze Beschreibung der verarbeiteten personenbezogenen Daten aus (Anlage 1, Abschnitte 2.1 und 2.2).

Schritt 2: Unterschreiben Sie die Vereinbarung entweder in Papierform oder als PDF mittels einer qualifizierten elektronischen Signatur.

Schritt 3: Senden Sie den ausgefüllten und unterzeichneten Auftragsverarbeitungs-Vertrag an Konica Minolta:

- Als unterschriebenes PDF, per E-Mail an eshop@konicaminolta.de

- Alternativ in Papierform per Post an Konica Minolta Business Solutions Deutschland GmbH, Europaallee 17, 30855 Langenhagen, Deutschland

Für weitere Fragen zu diesem Thema wenden Sie sich bitte an eshop@konicaminolta.de.

KONICA MINOLTA

Auftragsverarbeitungs-Vertrag

gem. Art. 28 DSGVO

zwischen

Kunde

Adresse

Stadt

als Verantwortlicher gem. DSGVO

und

Konica Minolta Business Solutions Deutschland GmbH
Europaallee 17
30855 Langenhagen

als Auftragsverarbeiter gem. DSGVO

Datum:

Version: 2026-06-02 BD DE web

Giving Shape to Ideas

§ 1 Vertragsgegenstand

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen auf Grundlage einer hauptvertraglichen Vereinbarung (z. B. Rahmenvertrag, Einzelbeauftragung, Smart Managed Services Vertrag, SaaS- oder Hosting-Vertrag, Miet- oder Leasingvertrag, Wartungsvertrag, Ausschreibung). Dieser Vertrag wird im Folgenden als „Hauptvertrag" bezeichnet. Insofern es sich bei den erbrachten Leistungen um Auftragsverarbeitung von personenbezogenen Daten handelt, schließen die Parteien zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten den vorliegenden Auftragsverarbeitungs-Vertrag („AVV").

(2) Die Art der verarbeiteten personenbezogenen Daten des Verantwortlichen, die Kategorien der von der Verarbeitung betroffenen Personen sowie Art und Zweck der Verarbeitung werden in **Anlage 1** näher spezifiziert.

(3) Die Dauer der Datenverarbeitung und die Laufzeit dieses AVV richten sich nach der Laufzeit des Hauptvertrags bzw. bestehen so lange fort, wie es die gesetzlichen Bestimmungen erfordern. Weitere Verpflichtungen oder Kündigungsrechte können sich aus den übrigen Bestimmungen dieses AVV ergeben.

§ 2 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mindestens in Textform). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Im Zusammenhang mit Weisungsbefugnissen ggf. zu bestimmende Personen werden in Anlage 1 definiert.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

(4) Weisungen des Verantwortlichen, die über die hauptvertraglich geschuldeten Leistungen und die hierzu erforderlichen Datenverarbeitungen hinausgehen und zu deren

Umsetzung der Auftragsverarbeiter auch nicht gesetzlich verpflichtet ist, könnten einer gesonderten Vergütung unterliegen.

§ 3 Schutzmaßnahmen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Er wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gemäß Art. 32 DSGVO, insbesondere mindestens die in **Anlage 1** aufgeführten Maßnahmen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(2) Der Auftragsverarbeiter benennt einen betrieblichen Datenschutzbeauftragten. Die Kontaktdaten des Datenschutzbeauftragten werden stets aktuell auf den Internetseiten des Auftragsverarbeiters veröffentlicht sowie der zuständigen Datenschutz-Aufsichtsbehörde mitgeteilt.

(3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrags betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrags oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragsverarbeiter bestehen bleiben.

§ 4 Pflichten des Auftragsverarbeiters

(1) Bei Verletzungen des Schutzes personenbezogener Daten des Verantwortlichen wird der Auftragsverarbeiter den Verantwortlichen unverzüglich in Schriftform oder Textform informieren. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten des Verantwortlichen enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragsverarbeiter wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Verantwortlichen liegt.

(5) Der Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gemäß Art. 30 Abs. 2 DSGVO enthält.

(6) Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 5 Rechte des Verantwortlichen

(1) Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Zertifizierungen und Testate von Sachverständigen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung (mindestens drei Wochen im Voraus) zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen. Prüfungen durch Dritte sind im Einvernehmen mit dem Auftragsverarbeiter abzustimmen. In einem Wettbewerbsverhältnis stehende Dritte kann der Auftragsverarbeiter ablehnen. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht

unverhältnismäßig stören. Jede Seite trägt die jeweils eigenen anfallenden Kosten des Audits.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

(3) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen schriftlich oder in Textform mit.

(4) Der Verantwortliche beurteilt die Zulässigkeit der Datenverarbeitung.

§ 6 Einsatz von Unter-Auftragsverarbeitern

(1) Die hauptvertraglich vereinbarten Leistungen bzw. die in **Anlage 1** beschriebenen Teilleistungen werden unter Einschaltung der jeweils produktspezifisch benannten Unter-Auftragsverarbeiter (”Subunternehmer”) durchgeführt.

(2) Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Veränderung bestehender oder Begründung neuer Unter-Auftragsverhältnisse (”Subunternehmerverhältnis”) befugt. Er setzt den Verantwortlichen hiervon unverzüglich in Kenntnis. Der Verantwortliche kann gegen die Hinzuziehung oder die Ersetzung von Subunternehmern Einspruch erheben. Der Verantwortliche hat einen etwaigen Einspruch unverzüglich zu erheben, er darf nicht auf sachfremden Erwägungen beruhen.

(3) Der Auftragsverarbeiter ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieses AVV zu verpflichten. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standardvertragsklauseln).

(4) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne

konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste.

§ 7 Anfragen und Rechte Betroffener

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie 32 bis 36 DSGVO.

(2) Sollte sich eine betroffene Person zwecks Geltendmachung ihrer Betroffenenrechte etwa auf Auskunftserteilung, Berichtigung oder Löschung ihrer Daten unmittelbar an den Auftragsverarbeiter wenden, so reagiert der Auftragsverarbeiter nicht selbstständig. Der Auftragsverarbeiter informiert – sofern der zuständige Verantwortliche aus dem Ersuchen zu ermitteln ist – den Verantwortlichen und wartet dessen Weisungen ab.

§ 8 Haftung

(1) Die Haftung folgt den gesetzlichen Vorschriften, maßgeblich denen des Art. 82 DSGVO.

§ 9 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen.

(2) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Der vorliegende AVV bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 10 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragsverarbeiter i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieses AVV bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Die Regelungen dieses AVV und seiner Anlagen gehen im Zweifel den Regelungen des Hauptvertrags vor.

(4) Sollten einzelne Bestimmungen dieses AVV ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(5) Gerichtsstand ist Hannover.

Unterschriften

Datum:	Datum: 09.07.2026
Für den Verantwortlichen:	Für Konica Minolta:
Name:	Name: Werner Theißen
Position:	Position: President, Managing Director

Datum:

Für den Verantwortlichen:

Name:

Position:

(Unterschrift einer zweiten Person nur falls die Geschäftsform des Verantwortlichen dies erfordert.)

Anlage zum Konica Minolta AVV

Version: 2026-06-01 BD MFP DE web

Beschreibung der produktspezifischen Auftragsverarbeitung in

Service & Wartung

Multifunktions- (MFP) &

Production Printing-Systeme

1. Beschreibung von Art und Zweck der Verarbeitung

Multifunktions- und Production Printing-Systeme der Marke Konica Minolta können papierne und elektronische Dokumente temporär speichern und zum Zwecke des Druckens, Scannens, Kopierens und Faxens elektronisch verarbeiten.

Konica Minolta erbringt im Auftrag des Verantwortlichen gemäß der hauptvertraglichen Vereinbarung oder einer späteren Einzelbeauftragung Serviceleistungen zur Bereitstellung, Inbetriebnahme, Instandhaltung, Wartung und Datenlöschung dieser Systeme.

Die vorliegende Anlage zum Vertrag zur Auftragsverarbeitung beschreibt die – zur Erbringung von Serviceleistungen an den Systemen erforderlichen – Verarbeitungen personenbezogener Daten durch Konica Minolta als Auftragsverarbeiter.

Die Verarbeitung personenbezogener Daten des Verantwortlichen oder Dritter (im Folgenden gemeinsam bezeichnet als „personenbezogene Daten des Verantwortlichen“) durch Konica Minolta erfolgt hierbei ausschließlich im Rahmen der Erbringung von Serviceleistungen. Eine darüberhinausgehende Erhebung oder Nutzung personenbezogener Daten erfolgt nicht. Die spezifische Art der

Verarbeitung erfolgt abhängig von den gewählten Service-Optionen und Remote Services. Unter Umständen wird der Verantwortliche während der Laufzeit des oder der Hauptverträge zwischen verschiedenen Service-Optionen wechseln.

Die Fernwartung von Konica Minolta Systemen kann entsprechend der gewählten Service-Variante (Remote Services) mittels der Konica Minolta Remote Service Platform („RSP"), über Remote-Panel sowie die Konica Minolta Lösungen „Konica Minolta Remote Support Tool" oder funktionsähnliche Lösungen erfolgen. Bei der Durchführung von Fernwartung lässt sich die Einsichtnahme in personenbezogene Daten des Verantwortlichen nicht ausschließen.

Konica Minolta Multifunktions- und Production Printing-Systeme sind dazu in der Lage, technische Vorgänge in verschlüsselten Log-Dateien zu erfassen. Die Erstellung von Log-Dateien wird seitens Konica Minolta erst dann initiiert, wenn Fehleranalysen notwendig werden. Die Log-Dateien können durch einen Konica Minolta Techniker vor Ort abgerufen werden, üblicherweise werden die Log-Dateien jedoch im Rahmen der Remote Services (bspw. „RSP") auf Konica Minolta Europe eigene Server (Server-Standort Deutschland) übertragen.

Außerdem können im Rahmen der Remote Services Sicherungskopien der Geräte-Konfiguration erstellt werden, die passwortgeschützt und verschlüsselt nach Wahl des Verantwortlichen auf eigenen oder Konica Minolta Europe Servern (Server-Standort Deutschland) gespeichert werden.

Sowohl Log-Dateien als auch Sicherungskopien der Geräte-Konfiguration enthalten keine Inhalte der auf dem Gerät verarbeiteten Druck-, Scan-, Kopier- oder vergleichbaren Vorgänge.

In sehr seltenen Fällen kann es erforderlich werden, dass Konica Minolta den Inhalt eines Gerätespeichers temporär auf einem anderen Datenträger zwischenspeichert, um den Gerätespeicher ohne Datenverlust reparieren oder ersetzen zu können. Der Verantwortliche kann hierbei ein externes Speichermedium zur Übertragung der Daten zur Verfügung stellen.

Im Falle einer eventuellen Geräterücknahme nach Vertragsende wird der Speicher des übernommenen Gerätes nach Maßgabe einer gesondert zu treffenden Vereinbarung entweder zerstört, gelöscht oder ausgebaut und dem Verantwortlichen übergeben. Dabei verarbeitet Konica Minolta möglicherweise personenbezogene Daten des Verantwortlichen, dies jedoch ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

Darüber hinaus ergeben sich Umfang und Zweck der Datenverarbeitung durch Konica Minolta aus dem Hauptvertrag bzw. eventuellen Zusatzvereinbarungen.

2.1 Art personenbezogener Daten

Personenbezogene Daten, die in Sicherungskopien der Geräte-Konfiguration enthalten sein können:
Geräte-Adressbuch (IT-Benutzernamen und Email-Adressen), IP-Adressen, MAC-Adressen, Seriennummer

Personenbezogene Daten, die in Log-Dateien maximal enthalten sind:
IT-Benutzernamen (z. B. Windows-Benutzernamen der Benutzer des Gerätes), Benutzer-Email-Adressen, IP-Adressen, MAC-Adressen, Seriennummer, Verlauf des geräteeigenen Browsers (aufgerufene Adressen), Verlauf des Gerätestatus, Verlauf der maximal letzten 150 Druckaufträge (Besitzer des Druckauftrags, Zeitstempel, Dokumentenname).

Alle in Log-Dateien erfassten Daten werden erst beginnend mit Initiierung der Erstellung einer Log-Datei erhoben, weiterhin werden alle o.g. Verläufe mit Ausschalten eines Gerätes gelöscht.

Personenbezogene Daten, die durch Konica Minolta Techniker im Rahmen von Bereitstellung/Inbetriebnahme bzw. Service & Wartung der Systeme möglicherweise verarbeitet werden:
[Diese Inhalte werden abhängig von den auf den eingesetzten MFP-Systemen verarbeiteten Inhalten durch den Verantwortlichen wie folgt bestimmt:]

☐ Personenstammdaten (z.B. Vorname und Nachname)
☐ Kommunikationsdaten (z.B. Telefonnummer, E-Mail Adresse)
☐ Vertragsdaten (Vertragsdokumente, Produkt- bzw. Vertragsinteresse)
☐ ERP- und/oder CRM-Inhalte
☐ Personalverwaltungsdaten
☐ Zahlungsdaten (Kontodaten, Kreditkartendaten)
☐ Informationen über Dritte (von Auskunfteien, aus öffentlichen Verzeichnissen)
☐ Benutzer-Identifikatoren (Benutzernamen, UIDs, etc.)
☐ Netzwerk-Identifikatoren (IP- & MAC-Adressen, IMEIs, etc.)

☐ Besondere Kategorien gem. Art. 9 DSGVO (wie im Folgenden angegeben):

☐ Weitere Arten personenbezogener Daten gem. Art. 4 Nr. 1 DSGVO, bzw. weitere spezifische Ausführungen zur Verarbeitung:

2.2 Kategorien betroffener Personen

[Die Kategorien der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen bestimmen sich nach der Art der Daten in Ziffer 2.1 und werden vom Verantwortlichen wie folgt festgelegt:]

☐ Beschäftigte (Art. 88 DSGVO)
☐ Geschäftspartner (Kunden, Lieferanten, inkl. Interessenten, Ansprechpartner)
☐ Minderjährige (als Endkunden, Beschäftigte, Familienangehörige, u. ä.)
☐ Weitere Kategorien bzw. spezifische Ausführungen:

3.1 Allgemeine Unter-Auftragsverarbeiter – beteiligt an jeder Verarbeitung

Konica Minolta Business Solutions Europe GmbH
Europaallee 17
30855 Langenhagen
Deutschland

Beschreibung der Teilleistung:

- IT-Service-Provider für Konica Minolta Business Solutions Deutschland (inkl. Betrieb der Konica Minolta Fernwartungs- und Sicherungs-Server)
- 2nd Level Service & Support für Konica Minolta Business Solutions Deutschland

Konica Minolta, Inc.
JP Tower

2-7-2 Marunouchi
Chiyoda-ku
Tokio
Japan

Beschreibung der Teilleistung:

- 3rd Level Support: In **seltenen Fällen** wird die Entwicklungsabteilung der Konica Minolta, Inc. zwecks Analyse unvorhergesehenen technischen Verhaltens hinzugezogen werden. Eine selbständige Zugriffsmöglichkeit durch die Konica Minolta, Inc. besteht jedoch zu keinem Zeitpunkt. Die Datenübermittlung erfolgt ausschließlich durch den europäischen Konica Minolta Support.

Beschreibung der Rechtsgrundlage der Drittstaatenübermittlung:

- Die Datenübermittlung an Konica Minolta, Inc. erfolgt auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission gem. Art. 45 DSGVO für Japan. Japan gilt insofern als „sicheres Drittland".

BLG Handelslogistik GmbH & Co. KG
Eduard Schopf Allee 1
28217 Bremen

Beschreibung der Teilleistung:

- Betrieb des Zentrallagers von Konica Minolta sowie Vorkonfiguration, Rücknahme und Entsorgung von Systemen

Service-Partner: In einigen Postleitzahl-Regionen Deutschlands werden Service & Wartung an Konica Minolta Systemen durch zertifizierte Partner erbracht. Diese Partner sind unter https://www.konicaminolta.de/de-de/support/service-partner einzusehen.

3.2 Anwendungsbezogene Unter-Auftragsverarbeiter – Nur bei Verwendung der folgenden speziellen Software-Lösungen

Software: SafeQ 6

Y Soft Corporation A.S.
Technická 2948/13
616 00 Brünn
Tschechische Republik

Beschreibung der Teilleistung:

- **Konica Minolta Deutschland oder Konica Minolta Europe können zwecks Analyse unvorhergesehenen technischen Verhaltens der Secure Print Lösung „SafeQ“ den Entwickler Y Soft hinzuziehen.**
- In Fall einer on-premises Installation (einschließlich eigener Cloud-Instanz des Verantwortlichen) kann es dafür notwendig sein, dass der Auftragsverarbeiter nach Rücksprache mit dem Verantwortlichen aktuelle Logfiles sowie störungsrelevante Informationen der SafeQ-Installation des Verantwortlichen an Y Soft übermittelt. Sollten Fernzugriffe durchgeführt werden, so können diese nur mit aktiver Bestätigung durch den jeweiligen Betreiber der Lösung SafeQ (den Verantwortlichen) erfolgen.
- Abweichend hiervon kann eine gesonderte Vereinbarung getroffen werden, die den dauerhaften Zugriff regelt. Ein solcher Zugriff kann nur durch den Verantwortlichen eingerichtet werden.

Software: AutoStore, ControlSuite, Printix, Power PDF

Tungsten Automation Ireland Ltd. [vormals „Kofax“]
70 Sir John Rogerson’s Quay
Dublin Docklands, Dublin 2
Irland

Beschreibung der Teilleistung:

- **Konica Minolta Deutschland oder Konica Minolta Europe können zwecks Analyse unvorhergesehenen technischen Verhaltens der Lösungen „AutoStore”, “ControlSuite”, “Printix”, und “Power PDF“ den Entwickler Tungsten Automation hinzuziehen.**
- Sollte hierzu die Übermittlung von Log-Dateien, die personenbezogene Daten enthalten, erforderlich werden, so wird hierzu ein SFTP-Server verwendet, auf den ausschließlich aus EU-Staaten und sicheren Drittstaaten gem. Art. 45 DSGVO zugegriffen werden kann.

Software: Document Navigator

Scanshare Applications B.V.
Hoofdstraat 7
5461 JC Veghel
Die Niederlande

Beschreibung der Teilleistung:

- **Konica Minolta Deutschland oder Konica Minolta Europe können zwecks Analyse unvorhergesehenen technischen Verhaltens der Lösung „Document Navigator“ den Entwickler Scanshare Applications hinzuziehen.**

- In Fall einer on-premises Installation kann es dafür notwendig sein, dass der Auftragsverarbeiter nach Rücksprache mit dem Verantwortlichen aktuelle Logfiles sowie störungsrelevante Informationen der Document Navigator Installation des Verantwortlichen an Scanshare Applications übermittelt. Sollten Fernzugriffe durchgeführt werden, so können diese nur mit aktiver Bestätigung durch den jeweiligen Betreiber der Lösung Document Navigator (den Verantwortlichen) erfolgen.
- Abweichend hiervon kann eine gesonderte Vereinbarung getroffen werden, die den dauerhaften Zugriff regelt. Ein solcher Zugriff kann nur durch den Verantwortlichen eingerichtet werden.

4. Technische und organisatorische Maßnahmen

1. Vertraulichkeit

a) Zutrittskontrolle

- Definition zutrittsberechtigter Personen mittels organisatorischer Festlegung
- Dokumentation der Vergabe und des Entzugs von Zutrittsberechtigungen
- Regelmäßige Auditierung der Zutrittsberechtigungen
- Zutrittsregelungen für betriebsfremde Personen
- Dokumentation der Anwesenheit in den Serverräumen
- Abgeschlossenes Gelände mit Zutritt nur für berechtigte Personen
- Alarmsicherung und Videoüberwachung des Geländes sowie innerhalb des Gebäudes inkl. der Serverräume
- Zutrittskontrolle entweder mit personalisiertem Ausweis inklusive Lichtbild sowie Zutrittskarte mit Pin-Code oder
- mit personalisiertem Token, biometrischer Zutrittskontrolle (Fingerprint) und Vereinzelungsanlage

b) Zugangskontrolle

- Zugang zu Systemen erfolgt mit Authentifizierung durch individuelle Benutzerkennung und Passwort
- Verwendung komplexer Passwörter mit mindestens 12 Zeichen und mindestens 3 der folgenden Kriterien: Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen. Bei der Erstellung werden gewählte Passwörter gegen die jeweils aktuelle „Microsoft Banned Password List“ geprüft, um Wörterbuch-Angriffe und Angriffe mit kompromittierten Passwörtern zu verhindern.
- Ein Passwortwechsel nach Ablauf einer bestimmten Zeitspanne wird nicht mehr erzwungen. Dies entspricht den aktualisierten Best Practice Empfehlungen des deutschen BSI und des amerikanischen NIST.

- Verbot der Weitergabe von Passworten
- Protokollierung der vergebenen Zugriffsberechtigungen
- Begrenzung der Administrationszugriffe auf das Mindestmaß
- Schutz der Datenverarbeitungssysteme vor unerlaubten Zugriffen durch geeignete Firewallsysteme
- Automatische Sperrung von Systemen nach bestimmter Zeit der Nichtbenutzung

c) Zugriffskontrolle:

- Einschränkung von Zugangsberechtigungen eingeschränkt auf Tätigkeitsbereiche
- Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)
- Protokollierung von Berechtigungsänderungen
- Kontrollen von unberechtigten Zugriffsversuchen

d) Trennungskontrolle:

- Trennung zwischen Administratoren- und Benutzerprofilen
- Spezifische Zugriffsberechtigung entsprechend den Anforderungen zum Zugriff auf die Daten
- Trennung von produktiven und Testsystemen durch technische Maßnahmen (virtuelle Server, getrennte Systeme, IP-Adress-Segmentierung)

2. Integrität

a) Weitergabekontrolle:

- Verschlüsselung bei der Übertragung von Daten, insbesondere bei der Übertragung über öffentliche Netze (z.B. SSL, TLS)
- Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken entsprechend einem Schutzklassenkonzept
- Verschlüsselung von Datenträgern
- Remote-Wipe Möglichkeit für mobile Endgeräte

b) Eingabekontrolle:

- Zugriffsrechte werden regelmäßig überprüft und aktualisiert
- Die Protokollierung von Datenbearbeitungen ermöglicht eine nachträgliche Überprüfung und Feststellung ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden (z.B. Datenänderungsprotokolle in zentralen ERP-Systemen)
- Aufzeichnung und bedarfsgerechtes Vorhalten von entsprechenden an Systemen durchgeführten Aktionen (z.B. Logfiles)
- Eindeutige Kennzeichnung der Datenspeicher aus den MFP/PP-Geräten bei Rücknahme

3. Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle und Wiederherstellbarkeit

- Nutzung zweier örtlich weit getrennter und zertifizierter Rechenzentren, die eine Betriebsunterbrechung mittels redundanter Datenhaltung verhindern
- Technische Vorkehrungen in Form von Frühwarnsystemen zum Schutz vor Störungen durch Feuer, Wasser oder überhöhte Temperaturen
- Maßnahmen gegen Stromausfall und -überlastung, z.B. Systeme zur unterbrechungsfreien Stromversorgung (USV)
- Planmäßige Durchführung von Datensicherungen, zus. Einsatz von Spiegelungsverfahren
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) durch globales systembezogenes Back-Up Konzept
- Mehrschichtige Virenschutz-/Firewall-Architektur
- Beschaffung von Hard- und Software durch zentralen IT-Anforderungs- und Beschaffungsprozess
- IT-Governance nach Cobit
- Regelmäßige Aktualisierung der verwendeten Systeme
- Notfallmaßnahmen- und Datenwiederherstellungsplan

4. Auftragskontrolle

- Bestellung eines Datenschutzbeauftragten
- Leistungsvereinbarungen mit sowie datenschutzkonforme Einschaltung von externen Dienstleistern
- Unterweisung der Mitarbeiter in der Verarbeitung personenbezogener Daten
- Verpflichtung der Mitarbeiter zur Vertraulichkeit über personenbezogene Daten
- Technische Absicherung durch Maßnahmen zur Zugriffs-, Trennungs- und Eingabekontrolle

5. Organisationskontrolle (Überprüfung, Bewertung und Evaluierung)

- Kontinuierliche Prozesse zur Überprüfung und ggf. Anpassung der Datenschutzmaßnahmen sind eingerichtet
- Schriftliche Regelung zum Kopieren von Daten
- Prozess zum Umgang mit einem Datenschutzvorfall
- Verarbeitung durch Mitarbeiter erfolgt nur auf dokumentierte Weisung der Geschäftsführung oder des jeweils Vorgesetzten
- Verbindliche Unternehmensrichtlinien zum Umgang mit personenbezogenen Daten sowie Nutzung von IT-Systemen
- Entsprechende Schulungen von Mitarbeitern
- Incident-Response-Management