Ratiodata AG | Auftrag zur Digitalisierung von Akten

Der Auftraggeber erteilt dem Geschäftsbereich Scan- & Dokumenten-Services der Ratiodata hiermit den Auftrag zur Digitalisierung von Akten zum Festpreis von 30 Euro je Akte*.

Das Angebot umfasst im Einzelnen

- Scannen des Ordnerinhalts
- Speicherung auf DVD im Datenformat PDF/A
- Erzeugung einer PDF-Datei pro Ordner
- Digitalisierung aller Papierbelege in den Formaten bis zu DIN A3 (Digitalisierung von Dokumenten in Überformaten bis DIN A0 als kostenpflichtige Option)

Folgende Leistungen werden von der Ratiodata erbracht

- Entfernung von Büroklammern, Ösen, Bindungen sowie Klarsichthüllen
- Doppelseitige Digitalisierung (Vorder- und Rückseite) in einer Auflösung von 200dpi
- Löschung leerer Rückseiten in einem automatisierten Verfahren
- Auslesen des Textinhalts der Dokumente mittels OCR-Verfahren und Einbetten in die PDF/A-Datei als Volltext
- Optional | Erfassung der Registerebenen der Akte mit Beschriftung jedes Registers (Register stehen in der Datei als Bookmark zur Verfügung)
- Datenschutzgerechte Vernichtung der Akten vier Wochen nach Daten-Bereitstellung

Kundendaten

Firma	
Name Ansprechpartner	
Vorname Ansprechpartner	
Straße und Hausnummer	
PLZ und Ort	
Telefon	
E-Mail	
Umsatzsteuer-ID (nur bei Firmenkunden)	
Anzahl Ordner	
Ansprechpartner Vertrieb Ratiodata (falls bekannt)	

* Standard-Akte bis zu 500 Blatt

Bereitstellung der Akten

☐ Zusendung durch den Auftraggeber

☐ Anlieferung durch den Aufraggeber (MO-FR von 06:00 bis 18:00 Uhr)

☐ Abholung (Kostenabstimmung im Einzelfall mit Ratiodata nach Transportart & Aufwand)

Digitalisierung der Akten

☐ Farbe

☐ S/W

☐ Dateiname gemäß Beschriftung des Ordnerrückens

☐ Dateiname gemäß Übergabeliste oder Excel-Tabelle (als Datei)

☐ Optional | Erfassung der Register (bis 10 Register je Ordner; je Ordner 4,50 €)

☐ Optional | Scannen von Formaten A2 bis A0 (je Dokument 1,00 €)

Datenbereitstellung per DVD

Beschriftung der DVD _____

Bitte tragen Sie hier den gewünschten Titel der DVD ein!

Rücklieferung

☐ Versand der DVD an den Auftraggeber (je Sendung 4,90 €)

Vernichtung*

☐ Ja, 4 Wochen nach Datenbereitstellung (je Ordner 0,50 €).

*Ohne Ihr Kreuz bei der Dokumentenvernichtung kann dieser Auftrag leider nicht verarbeitet werden. Stattdessen muss eine individuelle Abstimmung mit der Ratiodata stattfinden. Bitte nehmen Sie dazu Kontakt mit uns auf.

Mit Ihrer Auftragserteilung stimmen Sie der datenschutzgerechten Vernichtung Ihrer Dokumente zu. Sie erhalten keine gesonderte Vernichtungsvereinbarung. Die Auftragsabwicklung erfolgt auf Basis unserer Allgemeinen Geschäftsbedingungen. Diese sind im Internetauftritt der Ratiodata verfügbar.

Die im Anhang zu findende Vereinbarung zum Datenschutz und zur Datensicherheit gemäß §11 BDSG (ADV) wird Bestandteil dieses Auftrags zur Digitalisierung von Akten. Bitte geben Sie vor Erteilung des Auftrags in der ADV auf der zweiten Seite des Anhangs noch die Art der Daten und den betroffenen Personenkreis an.

Alle aufgeführten Preise verstehen sich zzgl. der gesetzlichen Mehrwertsteuer. Unsere Rechnungen sind zahlbar innerhalb von 10 Tagen nach Rechnungsdatum ohne Abzug.

Auftrag erteilt |

_____

Stempel, Unterschrift, Datum

Interner Vermerk (wird von der Ratiodata ausgefüllt!)

KD-Nr.	
CRM-Nr.	
Job-Nr.	

MES ☐ ID

MES ☐ Arbeitsgänge

☐ RD-Innenauftrag

☐ Jobneuanlage

☐ SAP-Referenzauftrag angelegt _____

☐ Fakturaregeln angelegt

Vereinbarung Auftragsverarbeitung

zwischen

Name der Firma

Straße der Firma

PLZ Ort – Sitz der Firma

- im Folgenden als **Verantwortlicher** bezeichnet -

und

Ratiodata AG
Gustav-Stresemann-Weg 29
48155 Münster

- im Folgenden als **Auftragsverarbeiter** bezeichnet –

- Auftragsverarbeiter oder Verantwortlicher jeweils als **Partei** und gemeinsam als die **Parteien** bezeichnet -

RATIODATA

Inhaltsverzeichnis

1. Gegenstand und Dauer des Auftrags 3
2. Konkretisierung des Auftragsinhalts 3
3. Technisch-organisatorische Maßnahmen 4
4. Weisungsrechte des Verantwortlichen 5
5. Kontrollrechte des Verantwortlichen 6
6. Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten 6
7. Unterstützung des Verantwortlichen bei der Erfüllung eigener Pflichten 7
8. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters 8
9. Unterauftragsverhältnisse 8
10. Löschung und Rückgabe von personenbezogenen Daten und Datenträgern 10
11. Verhältnis zu anderen Vereinbarungen, Sonstiges 11
12. Kündigung 11
13. Verzeichnis der Vertragsanlagen 12
14. Unterschriften 12

1. Gegenstand und Dauer des Auftrags

1.1.

Der Gegenstand des Auftrags ergibt sich aus dem Auftrag zur Digitalisierung von Akten, der Bestandteil des Vertrags ist, auf den hier verwiesen wird (im Folgenden insgesamt als Auftrag bezeichnet).

1.2.

Der Auftragsverarbeiter verarbeitet auf Grundlage des jeweiligen Vertrages personenbezogene Daten ausschließlich im Auftrag für den Verantwortlichen und nach dessen Weisung. Dies umfasst auch die Erstellung von Sicherungskopien und die Durchführung von Migrationen im Rahmen technischer Weiterentwicklungen, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind sowie den Umgang mit Daten, die im Hinblick auf die Einhaltung gesetzlicher Pflichten der Parteien erforderlich sind.

1.3.

Die Dauer des Auftrags (Laufzeit) sowie die Bedingungen für seine Beendigung ergeben sich aus dem jeweiligen Vertrag. Bestehen mehrere Verträge so gilt diese Vereinbarung bis zum Ablauf des Vertrages mit der längsten Laufzeit.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem jeweiligen Vertrag. einschließlich weitere die Leistung beschreibende Dokumente im Rahmen des jeweiligen Vertrags.

2.2. Art der personenbezogenen Daten

In der Regel werden die folgenden Datenarten/-kategorien verwendet:

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien oder aus öffentlichen Verzeichnissen)
- ☐

2.3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen wird im jeweiligen Vertrag konkret benannt und umfasst insbesondere:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte i. S. d. § 3 Abs. 11 BDSG
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐

2.4. Ort der Verarbeitung

Die Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter erfolgt ausschließlich im Gebiet von Mitgliedstaaten der Europäischen Union.

3. Technisch-organisatorische Maßnahmen

3.1.

Beim Umgang mit personenbezogenen Daten haben sowohl der Verantwortliche als auch der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen (im Folgenden: ToM) zu treffen, um die Anforderungen nach Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO einzuhalten.

3.2.

Die Parteien haben sich im Vorfeld der Auftragsvergabe und vor der ersten Auftragsausführung über die getroffenen Maßnahmen und deren Wirksamkeit in geeigneter Weise abzustimmen. Ergibt sich ein Anpassungsbedarf, ist dieser einvernehmlich umzusetzen.

3.3.

Die ToM dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

3.4.

Bei der Ausgestaltung der ToM sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

a) Die nichtauftragsspezifischen technisch-organisatorischen Datenschutzmaßnahmen sind in der **Anlage 1 ToM-SdV** zu dieser Vereinbarung beschrieben und sind ein Bestandteil dieser.
b) Die auftragsspezifischen technisch-organisatorischen Datenschutzmaßnahmen, sofern vorhanden ergeben sich aus dem jeweiligen Vertrag, einschließlich weitere die Leistung beschreibende Dokumente.

3.5.

Die ToM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Änderungen an den ToM, deren Auswirkungen unwesentlich für den Kontroll- und oder Sicherheitszweck sind, d.h. insbesondere das Sicherheitsniveau der vereinbarten Maßnahmen nicht unterschreiten, führt der Auftragsverarbeiter durch und informiert den Verantwortlichen hierzu auf Anfrage.

4. Weisungsrechte des Verantwortlichen

Der Verantwortliche bleibt für die Zulässigkeit der Verarbeitung der personenbezogenen Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Eine Verarbeitung der personenbezogenen Daten außerhalb der Zweckbestimmung des jeweiligen Vertrages ist dem Auftragsverarbeiter nicht gestattet. D. h. der Auftragsverarbeiter handelt ausschließlich nach Auftrag und Weisung des Auftraggebers.

4.1. Weisung

Weisungen des Verantwortlichen bedürfen grundsätzlich der Schriftform. Mündlich erteilte Weisungen bestätigt der Verantwortliche unverzüglich, mindestens in Textform. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

4.2. Aussetzung der Weisung

Der Auftragsverarbeiter hat das Recht, Weisungen des Verantwortlichen dann nicht auszuführen, wenn diese die Sicherheit der Verarbeitungen im Gesamten oder im Einzelfall gefährden könnten. Der Verantwortliche ist darüber unverzüglich zu informieren. Die Weisungen sind daraufhin in gegenseitigem Benehmen anzupassen oder zu verwerfen.

4.3. Änderung der Weisung durch Vertragsänderung

Änderungen des Verarbeitungsgegenstandes und Vertragsänderungen sind gemeinsam abzustimmen und zu dokumentieren. Vereinbarungen zu Leistungsänderungen im jeweiligen Vertrag finden auf Weisungen entsprechende Anwendung.

4.4. Verarbeitung aufgrund gesetzlicher Regelungen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten in Zusammenhang mit dem jeweiligen Vertrag auch, sofern er durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet ist.

5. Kontrollrechte des Verantwortlichen

5.1.
Der Verantwortliche hat das Recht eine Auftragskontrolle, die in der Regel rechtzeitig anzumelden ist, bei dem Auftragsverarbeiter zu den üblichen Geschäftszeiten und unter Begleitung in dessen Geschäftsräumen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Dies umfasst auch Stichprobenkontrollen.

5.2.
Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu erteilen und die entsprechenden Nachweise im Rahmen der gesetzlichen Möglichkeiten verfügbar zu machen.

5.3.
Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der ToM nachzuweisen.

5.4.
Der Nachweis der Wirksamkeit der ToM durch den Auftragsverarbeiter, die nicht nur den konkreten Auftrag betreffen, erfolgt grundsätzlich durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung anhand anerkannter Standards durch IT-Sicherheits- oder Datenschutzauditunternehmen (z.B. nach BSI-Grundschutz).

5.5.
Für die Ermöglichung von darüber hinaus gehenden Kontrollen durch den Verantwortlichen und die Bereitstellung von abweichend der in 5.4 genannten Informationen kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

6. Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten

6.1.
Der Auftragsverarbeiter hat personenbezogene Daten, die im Auftrag verarbeitet werden, nur nach Weisung zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken.

6.2.
Soweit ein Betroffener sich diesbezüglich unmittelbar an den Auftragsverarbeiter wenden sollte, wird er dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Ungeachtet dessen unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Bearbeitung des Vorgangs in angemessenem Umfang und stellt sämtliche relevanten Informationen unverzüglich zur Verfügung. Dies gilt auch für den Fall, der Geltendmachung sonstiger Rechte nach Kapitel 3 DSGVO durch den Betroffenen.

6.3.
Übersteigen die Unterstützungsleistungen im Zusammenhang mit der Geltendmachung von Betroffenenrechten einen angemessenen Umfang, erstattet der Verantwortliche die Mehraufwendungen dem Auftragsverarbeiter auf Nachweis.

6.4.
Soweit vom vereinbarten Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

7. Unterstützung des Verantwortlichen bei der Erfüllung eigener Pflichten

7.1.
Die Parteien informieren sich gegenseitig unverzüglich über Datenschutzverletzungen oder Verstöße gegen in dieser Vereinbarung festgelegte Bestimmungen, die im Rahmen der Auftragserfüllung des Vertrags aufgetreten sind.

7.2.
Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 30 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Auskunftspflichten, Meldepflichten bei Datenschutzverstößen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) Meldungen von Datenschutzverstößen mit Risiken für den Betroffenen an die Aufsichtsbehörden binnen 72 Stunden. Die Meldepflicht des Auftraggebers bleibt davon unberührt.

b) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

c) die Verpflichtung, Datenschutzverstöße unverzüglich an den Verantwortlichen zu melden. Es genügt die Textform

d) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzungen

e) die Unterstützung des Verantwortlichen bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten im Sinne von Art. 30 Abs. 1 DSGVO, bezogen auf den zwischen den Parteien geschlossenen Vertrag

f) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der zuständigen Aufsichtsbehörde

g) die Unterstützung des Verantwortlichen, soweit dieser seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der

Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist

h) die Information des Auftragsverarbeiters an den Auftraggeber, wenn eine Datenschutzaufsichtsbehörde Kontrollhandlungen das Auftragsverhältnis betreffend vornimmt und die Information rechtlich zulässig ist.

7.3.

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Verantwortlichen zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

8. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

8.1.

Der Auftragsverarbeiter hat einen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß den gesetzlichen Anforderungen ausübt oder, sofern er nicht zur Bestellung verpflichtet ist, einen fachkundigen Ansprechpartner benannt.

8.2.

Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

8.3.

Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

8.4.

Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO erfolgt gemäß 3.4 dieser Vereinbarung.

8.5.

Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

9. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

9.1. Haupt- und Nebenleistungen

Nicht zu den Hauptleistungen gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, sonstige Infrastrukturdienstleister, Post und Kurierdienste, Transportdienstleistungen, Sicherheits- und Reinigungsdienste sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Dies gilt ebenso bei einer rein technischen Wartung, die nicht zu einer Qualifikation als Auftragsverarbeiter und einer Anwendung von Art. 28 DSGVO führt.

Ist Auftragsgegenstand der (Fern-)Wartung der Umgang mit nicht anonymisierten oder pseudonymisierten und damit direkt erkennbaren personenbezogene Daten, insbesondere IBAN, BIC, Vorname und Name und oder strukturierten Datensätzen mit personenbezogenen Daten, so handelt es sich um eine Auftragsverarbeitung nach Art. 28 DSGVO.

Der Auftragsverarbeiter ist verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

9.2. Modalitäten der Unterbeauftragung

Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nach Unterzeichnung dieser Vereinbarung durch den Verantwortlichen unter den folgenden Bestimmungen einbinden:

a) Der Verantwortliche wird vorab über die Beauftragung weiterer Auftragsverarbeiter oder Datenempfänger informiert und kann der Beauftragung innerhalb einer Frist von 4 Wochen nach Zugang der Information widersprechen. Der Widerspruch kann entweder eine mögliche Beendigung des Vertrags oder, soweit es entsprechende alternative Auftragsverarbeiter gibt, die Übernahme der Zusatzkosten durch den Verantwortlichen zur Folge haben.

b) Der Auftragsverarbeiter hat den weiteren Auftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen dem Verantwortlichen und dem Auftragsverarbeiter getroffene Vereinbarung einhalten kann.

c) Die vertraglichen Vereinbarungen mit dem/den weiteren Auftragsverarbeitern sind so zu gestalten, dass sie den Datenschutzbestimmungen dieser Vereinbarung entsprechen. Insbesondere sind dem Verantwortlichen bzw. dessen dazu Beauftragten Kontroll- und Prüfungsrechte entsprechend dieser Vereinbarung beim weiteren Auftragsverarbeiter einzuräumen.

d) Der weitere Auftragsverarbeiter muss insbesondere hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts erfolgt. Der Nachweis erfolgt analog zu Punkt 5.4 dieser Vereinbarung gegenüber dem Auftragsverarbeiter.

e) Der Auftragsverarbeiter hat vorab und während der Vertragsdauer regelmäßig zu kontrollieren, dass der weitere Auftragsverarbeiter die nach den Vorgaben der DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Nachweis erfolgt analog zu Punkt 5.4 dieser Vereinbarung gegenüber dem Auftragsverarbeiter.

f) Der Auftragsverarbeiter ist berechtigt, den weiteren Auftragsverarbeitern zu gestatten ihrerseits weitere Auftragsverarbeiter (z. B. Konzerngesellschaften) vertraglich einzubinden. Voraussetzung für die weitere Unterbeauftragung ist die Gewährleistung des weiteren Auftragsverarbeiters, dass die Unterbeauftragung nur insoweit erfolgt, wie ein angemessenes Schutzniveau umgesetzt ist und die Anforderungen gemäß dieser Vereinbarung erfüllt sind.

g) Erbringt der weitere Auftragsverarbeiter die vereinbarte Leistung außerhalb der EU, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Hierzu beauftragt der Verantwortliche hiermit den Auftragsverarbeiter, mit weiteren Auftragsverarbeitern (insbesondere im Falle von Hardwarewartungs-, Softwarepflege und Supportleistungen, siehe auch Punkt 9.1 Abs. 3), soweit erforderlich, „EU-Standardvertragsklauseln“ bzw. deren rechtskonformen Nachfolgevereinbarungen abzuschließen.

h) Die Weitergabe von personenbezogenen Daten des Verantwortlichen an weitere Auftragsverarbeiter und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller oben genannten Voraussetzungen für eine Unterbeauftragung gestattet.

9.3. Haftungszurechnung

Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

10. Löschung und Rückgabe von personenbezogenen Daten und Datenträgern

10.1.

Vor Abschluss der vertraglichen Leistungen darf der Auftragsverarbeiter nicht mehr benötigte Daten erst nach vorheriger Zustimmung durch den Verantwortlichen löschen. Die Zustimmung kann auch durch eine Einigung der Vertragsparteien auf ein Löschkonzept erteilt werden. Test- und Ausschussmaterial ist unverzüglich datenschutzkonform zu vernichten bzw. zu löschen.

10.2.

Nach Aufforderung durch den Verantwortlichen, spätestens nach Abschluss der vertraglichen Leistungen, löscht bzw. vernichtet der Auftragsverarbeiter datenschutzkonform sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen. Besteht der Verantwortliche auf eine fortgesetzte Speicherung, trägt er die dadurch entstehenden Mehrkosten.

10.3.

Das Protokoll der Löschung bzw. Vernichtung ist auf Anforderung dem Verantwortlichen vorzulegen. Auf Anforderung und nach Abstimmung mit dem Verantwortlichen kann eine Herausgabe der Daten und Unterlagen an diesen erfolgen.

10.4.

Dokumentationen und Daten, die dem Nachweis der auftrags- und oder ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen gesetzlichen

oder vertraglichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann diese zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben, vernichten oder löschen.

10.5.
Kopien oder Duplikate der Daten, die im Rahmen des Vertrags verarbeitet werden, werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

11. Verhältnis zu anderen Vereinbarungen, Sonstiges

11.1.
Im Übrigen gehen die Regelungen dieser Vereinbarung im Zweifel den datenschutzrechtlichen Regelungen in den jeweiligen Verträgen und weiteren die Leistung beschreibenden Dokumenten vor. Dies gilt nicht für leistungsspezifische Regelungen bzw. konkrete Weisungen.

11.2.
Sollte Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren. Der Auftragsverarbeiter wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

11.3.
Für Nebenabreden zu dieser Vereinbarung ist die Schriftform erforderlich.

11.4.
Auf die Haftungsvereinbarung des jeweiligen Vertrages wird verwiesen.

11.5.
Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Vertragsparteien verpflichten sich, die unwirksamen Vertragsteile durch einvernehmlich getroffene wirksame Vereinbarungen zu ersetzen.

11.6.
Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss der Bestimmungen zum UN-Kaufrecht. Der Gerichtstand richtet sich nach den Regelungen des Vertrags.

12. Kündigung

12.1.
Das Kündigungsrecht richtet sich nach dem jeweiligen Hauptvertrag.

12.2.

Das Recht auf außerordentliche Kündigung aus wichtigem Grund bleibt unberührt.

13. Verzeichnis der Vertragsanlagen

Folgende Dokumente sind diesem Vertrag als Anlagen beigefügt:

Anlage 1: **ToM-SdV**
(Technisch-organisatorische Datenschutzmaßnahmen und Sicherheit der Verarbeitung)

Anlage 2: **Kontaktdaten und Subunternehmer**

14. Unterschriften

Ort, Datum	Ort, Datum
.....	……
(Unterschriften)	(Unterschriften)
Ratiodata AG	Firma
Namen in Klarschrift	Namen in Klarschrift

Anlage 1: ToM-SdV zur Vereinbarung Auftragsverarbeitung

Technisch-organisatorische Datenschutzmaßnahmen

und Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO

In Verbindung mit der Vereinbarung Datenschutz verpflichten sich die Vertragspartner in ihrem jeweiligen Verfügungsbereich und unter Berücksichtigung der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen nach dem Stand der Technik, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, zu implementieren. Die getroffenen Maßnahmen unterliegen einer regelmäßigen Prüfung ihrer Angemessenheit und Wirksamkeit.

Die vom Auftragsverarbeiter (AV) definierten und umgesetzten Maßnahmen dienen den datenschutzrechtlich geforderten Schutzzielen und sind im Wesentlichen wie folgt:

1. Vertraulichkeit
unter dem Aspekt der Kontrolle des berechtigten Zutritts:

Der unbefugte Zutritt zu Gebäuden, Räumen und Einrichtungen, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist zu verhindern.

Der AV hat umfangreiche bauliche, technische und organisatorische Maßnahmen umgesetzt, die den notwendigen Schutz vor dem unbefugten Eindringen in die Gebäude der Rechenzentren und Bürogebäude gewährleisten können.

Personell durch Pförtner und Sicherheitsdienste sowie technisch durch Videoanlagen überwacht der AV in den Rechenzentren den Zutritt auf das Betriebsgelände und in die Gebäude rund um die Uhr an allen Wochentagen.

An den Standorten sind Türen mit elektrischen Türschließsystemen versehen, die mit elektronischen Zutrittskarten geöffnet werden können. Besucher werden in den Gebäuden von Beschäftigten oder Sicherheitspersonal begleitet.

Für besondere Sicherheitsbereiche und zur Sicherstellung des Zugangs im Notfall werden entsprechende Sicherheitsschlüssel restriktiv und nachweisbar ausgegeben. Eine organisatorische Trennung von Bewilligung und technischer Umsetzung der Zutrittsberechtigung ist gegeben.

Einzelmaßnahmen sind insbesondere:

- Kartengestützte personalisierte Zutrittkontrollsysteme mit Zutrittsberechtigung nur für autorisierte Beschäftigte
- Dienstanweisungen zur Handhabung von Zutrittskontrollen
- Richtlinien zur Begleitung oder Kennzeichnung von Gästen im Gebäude
- Sicherheitszonen für Serverräume im Rechenzentrum sind mindestens durch 2 Faktor Authentifizierung gesichert
- Vergaberichtlinien für Zutrittsberechtigungen zu den Serverräumen
- Organisationsanweisung zur Ausgabe von Schlüsseln
- Regelung zum Umgang mit mobilen Endgeräten
- Gebäudesicherung durch Einbruchmeldeanlage und Wachdienst mit Kontrollgängen in Rechenzentren.

2. Vertraulichkeit
unter dem Aspekt der Kontrolle des berechtigten Zugangs:

Das Eindringen Unbefugter in Systeme und Anwendungen, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden, ist zu verhindern.

Um Zugang zu den technischen Systemen und Anwendungen des AV zu erhalten, muss ein Kennwort geschützter Benutzerstammsatz, das persönliche unternehmensweit gültige Benutzerkonto, technisch eingerichtet werden. Mit diesem authentifiziert sich der Nutzer gegenüber dem System oder der Anwendung.

Das Benutzerkonto muss beantragt und vom jeweiligen Vorgesetzten genehmigt werden. Der Bewilligungsprozess und die technische Benutzerkontenverwaltung sind organisatorisch getrennt.

Die Ausgestaltung, die Nutzung und den persönlichen Umgang mit dem Kennwort hat der AV in einer Passwortrichtlinie organisatorisch geregelt, deren Einhaltung technisch unterstützt wird. Darüber hinaus hat der AV auch den Gebrauch von Benutzerberechtigungen und den Umgang mit vertraulichen Daten geregelt.

Einzelmaßnahmen sind insbesondere:

- Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar
- Datenverschlüsselung bei Laptops, wenn Kundendaten verarbeitet werden
- Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar
- Sperrung des Benutzerkontos nach Überschreitung der Anzahl fehlgeschlagener Anmeldeversuche
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre nach 15 Minuten.
- Revisionssicheres, verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter
- Revisionssicheres, verbindliches Verfahren zur Vergabe von Berechtigungen
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten (z. B. „AZUBI1“)

- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passworten
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner)

3. Vertraulichkeit
unter dem Aspekt der Kontrolle des berechtigten Zugriffs:

Unerlaubte Tätigkeiten in DV-Systemen und mit DV-Anwendungen, die zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen, sind zu verhindern.

Zugriffsberechtigungen werden beim AV nach den Prinzipien "need-to-know" und "need-to-do" erteilt. Daher liegen den Zugriffsberechtigungen bedarfsorientierte Berechtigungskonzepte, Benutzerprofile und Funktionsrollen zugrunde.

Eine Zugriffsberechtigung wird auf Basis des Rollenkonzepts beantragt und vom Vorgesetzten genehmigt. In den Genehmigungsprozess sind weitere Kontrollinstanzen integriert. Zur technischen Zugriffssicherung verwendet der AV anerkannte Sicherheitssysteme, z.B. RACF oder Active Directory in Kombination mit TACACS

Zugriffe werden technisch überwacht. Die Ausführung administrativer Zugriffe wird protokolliert und kontrolliert. Auf die Anwendung bezogene Zugriffe werden mit den Mitteln und Möglichkeiten der Anwendung protokolliert und überwacht.

Einzelmaßnahmen sind insbesondere:

- Revisionskonformes, verbindliches Berechtigungsvergabeverfahren
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Vorgesetzten und Berechtigungsvergabe (technisch) durch IT-Abteilung
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(-gruppen)

4. Vertraulichkeit
unter dem Aspekt der Kontrolle der Zweck- und Mandantentrennung:

Daten verschiedener Verantwortlicher sind nach ihrem Erhebungszweck zumindest sachlogisch getrennt zu verarbeiten.

Der AV ist ein Mehrmandantendienstleister, Organisation, Systeme und Anwendungen sind speziell auf eine wirksame, zweckgebundene und mandantengetrennte Verarbeitung ausgerichtet. Test- und Produktionssysteme sind getrennt.

Einzelmaßnahmen sind insbesondere:

- Die Produkte und Leistungen stellen die nach Mandanten getrennte Datenverarbeitung sicher
- Es existiert ein Zugriffs- und Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Mandanten Rechnung trägt
- Grundsätzliche Trennung der Testsysteme und Anwendungen von den Produktionssystemen z.B. durch separate Hard- und Software
- Zugriffs- und Berechtigungskonzepte für Test- und Produktionsdaten und -systeme

5. Vertraulichkeit und Integrität
unter dem Aspekt der Kontrolle der Datenweitergabe:

Aspekte im Zusammenhang mit der Weitergabe personenbezogener Daten innerhalb und außerhalb der DV-Systeme und DV-Anwendungen sind zu regeln.

Die Vertraulichkeit und Weitergabe von personenbezogenen Daten, die außerhalb des Verfügungsbereichs des AV gelangen, werden einerseits durch Plausibilitätsprüfungen und oder Verifizierungsverfahren, andererseits durch die Verwendung von an die Erfordernisse angepasste und abgestufte Sicherheits- und oder Verschlüsselungsverfahren sichergestellt.

Firewallsysteme und ständig aktualisierte Virensoftware sichern neben einer Verschlüsselung nach dem Stand der Technik und dem Einsatz von VPN-Technologie die Kommunikation im Internet.

Einzelmaßnahmen sind insbesondere:

- Versand personenbezogener Daten, z. B. per verschlüsselter E-Mail
- Datenverschlüsselung
- Leitungsverschlüsselung (https, VPN etc.)
- Einsatz von Connect-Direct-Verbindungen zum Datenaustausch

6. Integrität
unter dem Aspekt der Kontrolle der Dateneingabe:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverarbeitung sind zu gewährleisten.

Eingaben in die Systeme und Anwendungen sowie deren Ausgaben werden vom AV generell protokolliert. Die Protokolle werden entsprechend den Inhalten und/oder gesetzlichen Vorgaben archiviert oder nach Zweckerreichung gelöscht bzw. für die weitere Verarbeitung gesperrt.

Einzelmaßnahmen sind insbesondere:

- Vertragliche Beschränkung des Umgangs mit personenbezogenen Daten des Verantwortlichen auf Beschäftigte des AV, die zur der vertraglich vereinbarten Leistungserbringung notwendig sind.
- Registrierung der Benutzer und User-ID bei der Anmeldung an die Systeme und Anwendungen in Verbindung mit der Protokollierung der Eingaben und Änderungen von und an Bestandsdaten
- Ggf. Bereitstellung von Protokollen zur Dateneingabekontrolle an den Verantwortlichen

7. Verfügbarkeit und „Belastbarkeit“
unter dem Aspekt der Kontrolle der Verfügbarkeit:

Personenbezogene Daten sind gegen zufällige oder mutwillige Zerstörung bzw. Verlust zu schützen.

Der AV betreibt ortsgetrennte Backup-Rechenzentren. Systeme sind gegen Angriffe von außen geschützt. Sie sind redundant ausgelegt und durch USV-Anlagen gesichert. Die Daten werden laufend gespiegelt. Eine permanente Überwachung der Auslastungen der Systeme sowie Maßnahmen zur Lastverteilung werden durchgeführt. Ein K-Fall-Konzept besteht. Die Funktionsfähigkeit wird regelmäßig getestet und das Ergebnis dokumentiert (s. a. Ziffer 3 und Ziffer 4).

Einzelmaßnahmen sind insbesondere:

- Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung
- Nachweis der sicheren und ordnungsgemäßen Archivierung in physisch geschütztem Archiv und verbindlicher Regelung der Zugriffsberechtigten
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutzkonzept usw.)
- Einsatz von Datenspiegelung
- Dopplung von Systemen, die für die Verarbeitung und Wiederherstellung der Betriebsbereitschaft unabdingbar sind.
- Einsatz unterbrechungsfreier Stromversorgung
- Laufende Lastverteilung und Performancemessung

- Ausgelagerte RZ-, Anwendungs- und Systemsteuerung sowie Netzüberwachung

8. Organisatorische Maßnahmen zu Verfahren unter dem Aspekt der regelmäßigen Überprüfung, Bewertung und Evaluierung:

Es ist seitens des Auftragsverarbeiters ein Datenschutzmanagementsystem zu implementieren, das geeignet ist, regelmäßig eine Überprüfung, Bewertung und Evaluierung der Einhaltung der datenschutzrechtlichen Anforderungen, insbesondere der technisch-organisatorischen Maßnahmen zu gewährleisten.

Weiterhin sind im Rahmen der Entwicklung und Bereitstellung von Hard- und Software die Datenschutzgrundsätze „privacy by design und default“ durch den Auftragsverarbeiter sicherzustellen.

Ein funktionsfähiges Incident- und Responsemanagement ist zu implementieren, das die zeitnahe Kommunikation über und nachhaltige Bearbeitung von Verstößen gegen datenschutzrechtliche Anforderungen dauerhaft ermöglicht.

Der AV führt Kontrollen zur Einhaltung der vertraglichen Regelungen zur Auftragsverarbeitung, die er mit den Verantwortlichen vereinbart hat, wirksam durch.

Der AV verarbeitet die ihm überlassenen Daten aufgrund und anhand von vertraglich vereinbarten Weisungen des Verantwortlichen gemäß den gesetzlich definierten Anforderungen zur Auftragsverarbeitung.

Aufgrund der hohen Bedeutung für den Verantwortlichen verfügt der AV über Prozesse und Verfahren, welche die Anforderungen an ein Datenschutzmanagementsystem, an ein Erkennungs- und Informationssystem bei Verstößen gegen datenschutzrechtliche Anforderungen, an die datenschutzkonforme Produkt- und Leistungser- sowie -bereitstellung und die regelmäßige Überprüfung, Bewertung sowie Evaluierung der Datenschutzprozesse und technisch-organisatorische Maßnahmen gewährleisten.

Kompetenzen und Kontrollmaßnahmen werden in Abstimmung mit dem Verantwortlichen definiert und technisch oder organisatorisch in die Betriebsabläufe eingebunden.

Einzelmaßnahmen sind insbesondere:

- Die vertraglichen Vereinbarungen enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Verantwortlichen
- Die vertraglichen Vereinbarungen enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Verantwortlichen sowie ein Verbot der Nutzung durch den AV außerhalb des schriftlich formulierten Auftrags und der Weisungen
- Die vertraglichen Vereinbarungen enthalten Regelungen zur Einbindung von weiteren Auftragsverarbeitern sowie deren Kontrollen durch den AV
- Der AV hat Prozesse zur sorgfältigen Auswahl, Einbindung und Kontrolle von weiteren Auftragsverarbeitern gemäß den datenschutzrechtlichen Anforderungen etabliert
- Der AV verpflichtet seine Beschäftigten, die in die Auftragsausführung eingebunden sind auf die Wahrung der Vertraulichkeit
- Der AV sensibilisiert die Beschäftigten zu datenschutzrechtlichen Anforderungen, insbesondere derjenigen, die für die ordnungsgemäße Auftragsverarbeitung erforderlich sind
- Der AV hat Regelungen getroffen, welche die bei der Auftragsausführung eingebundenen Beschäftigten zur Einhaltung der Aufträge und Weisungen des Verantwortlichen verpflichten
- Der AV hat vorwiegend technische Maßnahmen zur Zugriffssteuerung und -berechtigung auf personenbezogene Daten des Verantwortlichen wirksam implementiert.

  Diese gewährleisten, dass die Verarbeitung der Daten durch seine Beschäftigten im Rahmen der Aufgaben- und Auftragserfüllung oder aufgrund gesetzlicher Bestimmungen erfolgen.
- Der AV führt das erforderliche Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter und unterstützt den Verantwortlichen bei der Erfüllung seiner Dokumentationspflichten.
- Der AV beauftragt regelmäßig eine unabhängige Wirtschaftsprüfungsgesellschaft oder einen akkreditierten Zertifizierer mit der Prüfung und Bewertung der durchgeführten Kontrollmaßnahmen.

  Diese dokumentieren die Einhaltung der datenschutzrechtlichen Anforderungen eines Auftragsverarbeiters. Der AV stellt das Prüfungsergebnis den Verantwortlichen zur Verfügung.
- Der AV hat einen betrieblichen Datenschutzbeauftragten bestellt, der durch die Datenschutzorganisation effektiv in die relevanten betrieblichen Prozesse, auch in die zur Auftragsverarbeitung, einbezogen ist
- Der AV verfügt über eine Compliance-, IT-Sicherheits- und Revisions-Funktion und
- Der AV hat Informations- und Meldeprozesse etabliert, die eine Aufdeckung von Verstößen gegen die datenschutzrechtlichen oder vertraglichen Regelungen und eine diesbezügliche unverzügliche Kommunikation an den Verantwortlichen gewährleisten.
- Der AV hat intern und extern wirkende Prozesse zur Kommunikation mit dem Verantwortlichen etabliert, welche eine umfassende und abschließende Bearbeitung unter Einbindung aller Zuständigen sicherstellen kann.

Anlage 2: Kontaktdaten und Subunternehmer

1. Kontaktdaten zum Datenschutz des Auftragnehmers

Vorname und Name:	Dirk Warnke
Funktion:	Datenschutzbeauftragter
Tel.:	(069) 38076 – 2424
E-Mailadresse:	dirk.warnke@ratiodata.de

2. Aufstellung der Unterauftragnehmer

sofern im Gesamtleistungsumfang enthalten

Name	Anschrift	Auftragsinhalt
Rhenus SE & Co. KG	Rhenus-Platz 1 59439 Holzwickede	Entsorgung von elektronischen Datenträgern und Papier
Fiducia & GAD IT AG	Hahnstraße 48 60528 Frankfurt / Main	Technische Dienstleistungen / Entsorgung von elektronischen Datenträgern und Papier
Behinderten-Werke Main-Kinzig e.V.	Am Bahnhof 5a 63505 Langenselbold	Papierentsorgung am Standort Frankfurt
BüRe Dienstleistungen gGmbH	Kessler Weg 11 48155 Münster	Löschung und Vernichtung von Festplatten