**Vereinbarung zur Auftragsverarbeitung  
im Sinne des Art. 28 Abs. 3 DSGVO**

zwischen

Klicken oder tippen Sie hier, um Text einzugeben.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Klicken oder tippen Sie hier, um Text einzugeben.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Klicken oder tippen Sie hier, um Text einzugeben.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

– im Folgenden als **Verantwortlicher** bezeichnet –

und

**BankingGuide GmbH**

Fürstenwall 172

D-40217 Düsseldorf

– im Folgenden als **Auftragsverarbeiter** bezeichnet –

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

Inhalt

[1 Gegenstand und Dauer des Auftrags 3](#_Toc207636791)

[2 Konkretisierung des Auftragsinhalts 3](#_Toc207636792)

[3 Technisch-organisatorische Maßnahmen 5](#_Toc207636793)

[4 Weisungsrechte des Verantwortlichen 6](#_Toc207636794)

[5 Kontrollrechte des Verantwortlichen 7](#_Toc207636795)

[6 Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten 8](#_Toc207636796)

[7 Unterstützung des Verantwortlichen bei der Erfüllung eigener Pflichten 8](#_Toc207636797)

[8 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters 9](#_Toc207636798)

[9 Unterauftragsverhältnisse 10](#_Toc207636799)

[10 Löschung und Rückgabe von personenbezogenen Daten und Datenträgern 12](#_Toc207636800)

[11 Verhältnis zu anderen Vereinbarungen, Sonstiges 13](#_Toc207636801)

# Gegenstand und Dauer des Auftrags

1.1 Der Gegenstand des Auftrags ergibt sich aus Lizenzvertrag zwischen den Parteien (im Folgenden „Vertrag“).

1.2 Der Auftragsverarbeiter verarbeitet auf Grundlage des Lizenzvertrags 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 Lizenzvertrag.

# Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der Verarbeitung

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch („Fernwartung“). Darüber hinaus übernimmt der Auftragnehmer Aufgaben zur Durchführung von Änderungen an den fachlichen Einstellungen der Anwendung („Fachliche und technische Konfiguration“). Außerdem übernimmt der Auftragnehmer die Betreuung und Behebung von gemeldeten Auffälligkeiten und Fehlern („Support“). In diesem Zusammenhang ist es nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können. Etwaige Details ergeben sich aus dem Lizenzvertrag und weiteren die Leistung beschreibenden Dokumenten des Vertragspakets (z. B. IT-Sicherheitskonzept).

2.2 Art der personenbezogenen Daten

Es werden personenbezogene Daten der folgenden Datenarten/-kategorien verwendet:

* Personenstammdaten
* Kommunikationsdaten (z. B. Telefon, E-Mail)
* Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
* Informationen im Zusammenhang mit der Beratung
* Sonstige personenbezogene Daten, die ggf. einsehbar sind

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind:

* Kunden und Lieferanten
* Interessenten
* Ansprechpartner
* Sonstige Dritte, die ggf. einsehbar sind

2.4 Ort der Verarbeitung

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

oder

b) (nur auszufüllen, wenn 2.4 a) nicht zutrifft)

Eine Datenverarbeitung außerhalb dieses Gebiets bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau in: Vereinigte Staaten

☒ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission  
 (Art. 45 Abs. 3 DSGVO) ;

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften  
 (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO) ;

☒ wird hergestellt durch Standarddatenschutzklauseln  
 (Art. 46 Abs. 2 litt. c und d DSGVO) ;

☐ wird hergestellt durch genehmigte Verhaltensregeln  
 (Art. 46 Abs. 2 lit. e i.V.m. 40 DSGVO) ;

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus  
 (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO) ;

☐ wird hergestellt durch sonstige Maßnahmen (siehe Anlage)  
 (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DSGVO) ;

c) Die Verarbeitung und Nutzung der personenbezogenen Daten des Verantwortlichen erfolgt grundsätzlich in den Betriebsstätten des Auftragsverarbeiters. Die auch nur zeitweise erforderliche Erhebung oder Verarbeitung dieser Daten außerhalb der Betriebsstätten des Auftragsverarbeiters (z. B. Telearbeit, Remotezugriff etc.) ist gestattet, soweit der Auftragsverarbeiter

a. betriebliche oder einzelvertragliche Vereinbarungen mit seinen Beschäftigten getroffen hat, die den einschlägigen datenschutz- und datensicherheitsrechtlichen Bestimmungen genügen und die Beschäftigten zur Vertraulichkeit entsprechend Art. 28 Abs. 3, b DS-GVO verpflichten.

b. sich in diesen Vereinbarungen vorbehalten hat, bei Verdacht auf Missbrauch den Zugang, - und damit das Recht zur Verarbeitung personenbezogener Daten außerhalb der Betriebsstätte -, unverzüglich sperren zu können.

d) Im Falle des begründeten Verdachts der Nichteinhaltung der einschlägigen, datenschutz- und datensicherungsrechtlichen Bestimmungen wird der Verantwortliche dem Auftragsverarbeiter dies mitteilen. Der Auftragsverarbeiter wird daraufhin unverzüglich die notwendigen Maßnahmen ergreifen. Der Auftragsverarbeiter wird den Verantwortlichen von dem Ergebnis seiner Untersuchung und der getroffenen Maßnahmen in Kenntnis setzen.

# 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 herzustellen.

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 TOM-SdV zu dieser Vereinbarung beschrieben und sind ein Bestandteil dieser.

b) Die auftragsspezifischen technisch-organisatorischen Datenschutzmaßnahmen, sofern vorhanden ergeben sich aus dem Lizenzvertrag, einschließlich der weiteren die Leistung beschreibenden Dokumente, z.B. IT-Sicherheitskonzept.

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.

# 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 Vertrages ist dem Auftragsverarbeiter nicht gestattet.

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 so lange 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 Vertrag finden auf Weisungen entsprechende Anwendung.

4.4 Verarbeitung aufgrund gesetzlicher Regelungen

Der Auftragsverarbeiter verarbeitet personenbezogene Daten sofern er durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet ist.

# Kontrollrechte des Verantwortlichen

5.1 Der Verantwortliche und oder dessen Auftraggeber\* 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.  
  
\* Auftragsleistungen, die das Bankverfahren unmittelbar betreffen.

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.

# 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.

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.

# 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) 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

b) die Verpflichtung, Datenschutzverstöße unverzüglich an den Verantwortlichen zu melden

c) die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzungen

d) 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

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

f) 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

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

# 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 Falls der Auftragsverarbeiter seinen Sitz außerhalb der Union hat, benennt er einen Vertreter nach Art. 27 Abs. 1 DSGVO in der Union. Seine Kontaktdaten werden dem Verantwortlichen in geeigneter Weise zur Verfügung gestellt.

8.3 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.

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.

8.6 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

8.7 Personenbezogene Daten dürfen nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet werden, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

# 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, da die Kenntnisnahme von personenbezogenen Daten des Verantwortlichen abschließend ausgeschlossen werden kann.

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 begründete Widerspruch kann entweder eine mögliche Beendigung des Vertrags oder, soweit es entsprechende alternative Auftragsverarbeiter gibt, die Übernahme der etwaigen 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.

# 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.

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.

10.3 Dokumentationen und Daten, die dem Nachweis der auftrags- und oder ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen gesetzlichen oder vertraglichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann diese zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben, vernichten oder löschen.

10.4 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.

# Verhältnis zu anderen Vereinbarungen, Sonstiges

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

11.2 Für Nebenabreden zu dieser Vereinbarung ist die Schriftform erforderlich.

11.3 Auf die Haftungsvereinbarung des Vertrages wird verwiesen.

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

11.5 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

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.

11.7 Der Verantwortliche erkennt an, dass zur vollständigen Erbringung der vertraglich vereinbarten Leistungen die BMS Corporate Solutions GmbH als Unterauftragsverarbeiter eingesetzt wird. Die BMS Corporate Solutions GmbH übernimmt sämtliche Aufgaben im Rahmen der vereinbarten Leistungen. Aus diesem Grund sind für diese Leistungen die technischen und organisatorischen Maßnahmen der BMS Corporate Solutions GmbH relevant und beigefügt.

Die BMS Corporate Solutions übernimmt ferner Aufgaben der Entwicklung, Wartung und Verwaltung der Softwarelösungen für die BankingGuide GmbH.

Die BankingGuide GmbH hat mit der BMS Corporate Solutions GmbH eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO geschlossen. Die BankingGuide GmbH gewährleistet, dass die BMS Corporate Solutions GmbH die gleichen Verpflichtungen in Bezug auf Datenschutz und Datensicherheit erfüllt, wie sie in der vorliegenden Vereinbarung geregelt sind.

**BankingGuide GmbH**

Düsseldorf, 22.09.2025

Ein Bild, das Entwurf, Handschrift, Zeichnung, Kalligrafie enthält.

Automatisch generierte Beschreibung Ein Bild, das Handschrift, Schrift, Kalligrafie, Typografie enthält.

Automatisch generierte Beschreibung

……………………………………………. …………………………………………….

Dennis Liemann, Geschäftsführer Ralf Schneider, Geschäftsführer

Klicken oder tippen Sie hier, um Text einzugeben.

Klicken oder tippen Sie hier, um Text einzugeben. , 22.09.2025

……………………………………………. …………………………………………….

Klicken oder tippen Sie hier, um Text einzugeben. Klicken oder tippen Sie hier, um Text einzugeben.

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

Anlage 2: Kontaktdaten und Subunternehmer