BMS CONSULTING

Vereinbarung über die Wartung und Pflege von IT-Systemen im Sinne des Art. 28 Abs. 3 DSGVO

Stand: 01.01.2020

Inhaltsverzeichnis

Vereinbarung über die Wartung und Pflege von IT-Systemen

im Sinne des Art. 28 Abs. 3 DSGVO

zwischen

Klicken Sie hier, um Text einzugeben.

Klicken Sie hier, um Text einzugeben.

Klicken Sie hier, um Text einzugeben. - Klicken Sie hier, um Text einzugeben. Klicken Sie hier, um Text einzugeben.

- nachstehend „**Auftraggeber**“ genannt -

Und der

BankingGuide GmbH

Fürstenwall 172,

D-40217 Düsseldorf

- nachstehend „**Auftragnehmer**“ genannt -

Präambel

Zwischen den Parteien besteht ein Vertragsverhältnis über die Wartung und Pflege von IT-Systemen. Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben der Auftragsdatenverarbeitung nach Art. 28 DSGVO geschlossen.

1 Ausgangssituation

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch. In diesem Zusammenhang ist 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.

2 Gegenstand der Vereinbarung

Im Rahmen der Erfüllung obiger Aufgaben kann es erforderlich sein, dass ein Zugriff auf das betroffene System von außerhalb notwendig wird („Fernwartung“). Die folgende Vereinbarung regelt den datenschutzrechtlichen Rahmen dieses Zugriffs.

(1) Der Auftragnehmer übernimmt im Rahmen des Anwendungssupports und der bankindividuellen Anwendungsspezifikation Aufgaben zur Durchführung von Änderungen an den fachlichen Einstellungen der Anwendung (fachliche und technische Konfiguration) sowie die Betreuung und Behebung von gemeldeten Auffälligkeiten und Fehlern (Support).

(2) Zur Durchführung von Fernwartungen sind seitens des Auftragnehmers alle Mitarbeiter des Vertriebs, Supports, Produktmanagements und der Entwicklung berechtigt. Dies erstreckt sich auch auf die Mitarbeiter der in Anlage 2 – Genehmigte (Sub)unternehmer genannten Unternehmen.

(3) Ein Zugriff per Fernwartung erfolgt ausschließlich über dafür autorisierte gesicherte Softwarelösungen (siehe hierzu Anlage 3 - autorisierte Softwarelösungen) und nur nach vorheriger mündlicher, telefonischer oder schriftlicher Beauftragung durch den Auftraggeber.

(4) Eine Änderung der autorisierten Softwarelösungen ist nur möglich, sofern dies aus datenschutzrechtlichen Gründen notwendig ist. Die Änderung erfolgt in Abstimmung mit dem Auftraggeber.

(5) Der Auftragnehmer gewährleistet, dass bei allen involvierten Mitarbeitern eine hinreichende Sachkunde zur Durchführung benannter Aufgaben vorhanden ist.

3 Laufzeit und Kündigung

(1) Diese Vereinbarung richtet sich nach den Laufzeiten und Kündigungsfristen des Lizenzvertrages. Verstöße gegen die Verpflichtungen aus diesem Vertrag gelten auch als Verstöße gegen den Lizenzvertrag und können nach dessen Regelungen zu einer außerordentlichen Kündigung berechtigen.

(2) Mit Beendigung des Lizenzvertrages endet diese Vereinbarung automatisch, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten aus dieser Vereinbarung über die Auftragsdatenverarbeitung gelten in jedem Fall auch nach einer Beendigung des Lizenzvertrages bis zur vollständigen Vernichtung oder Rückgabe aller im Zusammenhang mit dem Lizenzvertrag stehenden Daten durch den Auftragnehmer. Auch über das Vertragende hinweg verpflichtet sich der Auftragnehmer unbefristet, die zur Kenntnis erlangten Daten vertraulich zu behandeln.

4 Konkretisierung des Auftraginhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im jeweiligen Lizenzvertrag.

(2) Art der personenbezogenen Daten

☐ Die Art der verwendeten personenbezogenen Daten nach Art. 4 Nr. 1, 13, 14 und 15 DSGVO ist im jeweiligen Lizenzvertrag konkret beschrieben.

☑ Gegenstand der Verarbeitung personenbezoger Daten sind folgende Datenarten/-kategorien (Aufzählung / Beschreibung der Datenkategorien)

- ☑ Personenstammdaten
- ☑ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☑ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Abrechnungsdaten
- ☑ Beratungsdaten ZV-Beratung

(3) Kategorien betroffener Personen:

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffenen Personen nach Art. 4 Nr. 1 DSGVO ist im Lizenzvertrag konkret beschrieben.

☑ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☑ Kunden / Lieferanten
- ☑ Interessenten
- ☐ Beschäftigte gem. § 26 Abs. 1 BDSG, Art. 88 Abs. 1 DSGVO
- ☐ Handelsvertreter
- ☑ Ansprechpartner
- ☐

(4) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über

den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 bis 50 DSGVO erfüllt sind.

(5) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, inbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

5 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen im Sinne der Artt. 5, 32 DSGVO vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber auf Verlangen zur Prüfung vorzulegen.

(2) Bei den zu treffenden Maßnahmen handelt es sich u.a. um Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Trennbarkeit, Pseudonymisierung, Weitergabekontrolle, Eingabekontrolle, Verfügbarkeitskontrolle, Wiederherstellbarkeit, datenschutzfreundliche Voreinstellung und Auftragskontrolle. (siehe hierzu ausführlich Anlage 4 - Technische und organisatorische Maßnahme der BMS Berens Mosiek Siemes Consulting GmbH)

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6 Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

7 Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32-36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und notwendigen vorherigen Konsultationen. Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28-33 DSGVO. Insbesondere gewährleistet er die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung – soweit gesetzlich nach Art. 37 DSGVO, § 38 BDSG vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38, 39 DSGVO, § 38 BDSG ausüben kann. Dessen Kontaktdaten werden den Auftragnehmer zum Zweck der direkten Kontaktaufnahme mitgeteilt. Gleichzeitig teilt auch der Auftraggeber dem Auftragnehmer die Kontaktdaten seines Datenschutzbeauftragten bzw. die Kontaktdaten seines Ansprechpartners für Datenschutz mit.

(2) Er gewährleistet gemäß Art. 28 Abs. 3 b) DSGVO, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen sowie über die bestehende Weisungs- bzw. Zweckbindung belehrt wurden. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Ferner

müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit mit Wirkung für die Zukunft fortbesteht.

(3) Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Artt. 5, 32 DSGVO und der Anlage „Technische und organisatorische Schutzmaßnahmen nach Artt. 5, 32 DSGVO."

(4) Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 51 DSGVO, § 40 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach den Artt. 83, 84 DSGVO bzw. §§ 41,42, 43 BDSG bei dem Auftragnehmer ermittelt.

(5) Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags. Die Auftragskontrolle des Auftragnehmers entbindet nicht den Auftraggeber von der eigenen Pflicht zur Auftragskontrolle.

(6) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer insbesondere auch aktuelle Testate, Berichte oder Berichtsauszüge (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) vorlegen. Der Nachweis solcher Maßnahmen kann ebenfalls u.a. erfolgen durch: die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8 Unterauftragsverhältnisse

(1) Die in „Anlage 2 – Genehmigte (Sub)unternehmer" genannten Subunternehmer sind für den Auftragnehmer gemäß der dort genannten Auftragsinhalte tätig. Mit der Beauftragung dieser Unterauftragnehmer erklärt sich der Auftraggeber einverstanden. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers sonstige Unterauftragnehmer einbezogen werden sollen, bedarf dies der vorherigen ausdrücklichen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer kommt seinen Verpflichtungen des Art. 28 Abs. 2-4 DSGVO bei der Unterbeauftragung nach Satz 1 und Satz 3 nach.

(2) Der Auftragnehmer hat die vertraglichen Vereinbarungen mit Unterauftragnehmern so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen. Die Weitergabe von personenbezogenen Daten des Auftraggebers bzw. des Auftragnehmers an Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen nach Abs. 1 gestattet. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(3) Im Falle der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, von dem Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

(4) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, gemäß § 28 Abs. 3, h) DSGVO Überprüfungen einschließlich Inspektionen beim Auftragnehmer durchzuführen. Der Auftragnehmer ermöglicht diese Überprüfungen und trägt dazu bei. Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in deren Geschäftsbetrieb zu überzeugen. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

10 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber unverzüglich eine Meldung, wenn aus der Sphäre des Auftragnehmers Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen erfolgt sind.

(2) Dem Auftragnehmer ist bekannt, dass nach Artt. 33, 34 DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Entsprechende Vorfälle hat der Auftragnehmer ohne Ansehen der Verursachung dem Auftraggeber unverzüglich mitzuteilen. Dies gilt auch bei etwaigen schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit dem Auftraggeber Pflichten nach Artt. 33, 34 DSGVO treffen, hat der Auftragnehmer diesen hierbei zu unterstützen.

11 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. Art. 28 Abs. 3, a) DSGVO). Im Rahmen der in dieser Zusatzvereinbarung getroffenen Auftragsbeschreibung behält sich der Auftraggeber ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, die er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(2) Mündliche Weisungen wird der Auftraggeber schriftlich oder per E-Mail (in Textform) bestätigen. Weisungsbefugte und weisungsempfangende Personen sind in Anlage 1 – Kontaktpersonen / Weisungsberechtigte definiert.

(3) Der Auftragnehmer verwendet die Daten für die im Hauptvertag bestimmten Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers 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.

(4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

12 Löschung von Daten und Rückgabe von Datenträgern

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt und sind streng untersagt. Hierfür bedarf es einer vorherigen schriftlichen Genehmigung des Auftraggebers. 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.

(3) Nach Abschluss der vertraglichen Arbeiten oder nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung des Lizenzvertrages – hat der Auftragnehmer sämtliche in seinem Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann diese zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13 Leistungsort

(1) Die Erbringung der in § 1 dargestellten Leistungen des Auftragnehmers erfolgt vor Ort beim Auftraggeber, durch die Mitarbeiter der BMS Berens Mosiek Siemes Consulting GmbH in Düsseldorf, in den Räumlichkeiten der in der Anlage 2 angegebenen Unternehmen oder in den Räumlichkeiten nachträglich durch den Auftraggeber genehmigter Subunternehmer.

14 Haftungserklärung

(2) Der Auftraggeber und der Auftragnehmer vereinbaren für die Durchführung dieses Auftrages, dass die Haftung des Auftragnehmers im Rahmen dieses Auftrages grundsätzlich auf vorsätzliches oder grob fahrlässiges Verschulden beschränkt ist.

(3) Der Auftraggeber und der Auftragnehmer vereinbaren für die Durchführung dieses Auftrages, dass die Haftung des Auftragnehmers im Rahmen dieses Auftrages auf eine Summe in Höhe von € 3.000.000 bei Personen- und Sachschäden und € 100.000 bei Vermögensschäden pro Schadensfall beschränkt ist. Die Vereinbarung einer höheren Haftungssumme ist von dem Auftraggeber aufgrund der damit verbundenen zusätzlichen Kosten für einen weitergehenden Versicherungsschutz des Auftragnehmers nicht gewünscht.

15 Wahrung von Geschäftsgeheimnissen

(1) Die Parteien verpflichten sich zu strikter Vertraulichkeit Dritten gegenüber. Insbesondere sind die Parteien verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekanntwerdenden Geschäfts- und Betriebsgeheimnisse, Herstellungsverfahren, Arbeitsmethoden und sonstigen geschäftlichen bzw. betrieblichen Tatsachen, Unterlagen und Informationen der anderen Partei sowie ihrer Kunden und Geschäftspartner streng vertraulich zu behandeln, in keiner Weise Dritten zugänglich zu machen oder sonst zu verwenden. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig. Die Parteien verpflichten sich zu strikter Vertraulichkeit Dritten gegenüber auf unbegrenzte Zeit.

(2) Die vorgenannte Verpflichtung findet insoweit keine Anwendung, als die Partei darlegen kann, dass diese Information

- öffentlich zugänglich und zum Zeitpunkt der Offenlegung verfügbar ist, oder danach der Öffentlichkeit zugänglich geworden ist und zwar ohne Verletzungshandlung oder -unterlassung durch diese Partei oder eines seiner Vertreter oder Angestellten, oder
- vor dem Erhalt von der anderen Partei im Besitz der Partei oder ihr bekannt war, oder
- der Partei durch eine andere Person ohne Einschränkung rechtmäßig offengelegt wurde, oder
- von der Partei ohne Zugang zur Information der anderen Partei unabhängig entwickelt wurde, oder
- nach gesetzlichen oder verwaltungsrechtlichen Vorschriften offengelegt werden muss, wenn der anderen Partei dieses Erfordernis unverzüglich bekannt gegeben wird und der Umfang solcher Offenlegung soweit wie möglich eingeschränkt wird, oder aufgrund einer gerichtlichen Entscheidung offengelegt werden muss, wenn der anderen Partei von dieser Entscheidung unverzügliche Nachricht gegeben wurde und wenn nicht die Möglichkeit besteht, diese Entscheidung anzufechten.

16 Kontaktpersonen

(1) Soweit Weisungen oder Hinweise nach dieser Vereinbarung gegenüber der anderen Partei zu erfolgen haben, sind diese an einen der in Anlage 1 – Kontaktpersonen / Weisungsberechtigte genannten Personen zu richten. In Vertretung sind auch dessen mit dieser Aufgabe betraute weisungsgebundene Mitarbeiter zum Empfang von Weisungen berechtigt.

(2) Jede Partei kann ihre im vorigen Absatz genannten Kontaktpersonen durch schriftliche Erklärung gegenüber der anderen Partei ändern.

17 Schlussbestimmungen und Unterschriften

(1) In dieser Zusatzvereinbarung sind sämtliche Rechte und Pflichten der Vertragsparteien geregelt. Änderungen oder Ergänzungen bedürfen der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Regelungen handelt.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen Vertragsbestimmungen soll eine angemessene Regelung treten, die dem erkennbaren Vertragswillen so weit wie möglich entspricht.

(3) Es gilt deutsches Recht. Ausschließlicher Gerichtsstand für beide Seiten ist Düsseldorf.

(4) Die Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1 – Kontaktpersonen / Weisungsberechtigte
- Anlage 2 – Genehmigte (Sub)unternehmer
- Anlage 3 - autorisierte Softwarelösungen
- Anlage 4 - Technische und organisatorische Maßnahme der BMS Berens Mosiek Siemes Consulting GmbH

Unterschriften Auftraggeber:

_____ , den _____
Ort, Datum

_____
Firmenstempel

_____
Unterschrift (en) Auftraggeber

_____ _____
Name (n) /Funktion in Klarschrift Name (n) /Funktion in Klarschrift

Unterschrift Auftragnehmer:
BankingGuide GmbH
Düsseldorf, den _____
Ort, Datum

_____
Firmenstempel

_____
Unterschrift Auftragnehmer

Dennis Liemann / Geschäftsführer
Name/Funktion in Klarschrift

18 Anlagen

18.1 Anlage 1 – Kontaktpersonen / Weisungsberechtigte

Folgende Personen sind berechtigt, dem Auftragnehmer – die Auftragsverarbeitung betreffend - Weisungen zu erteilen und sämtliche auftragsbezogene Entscheidungen zu kommunizieren und Abnahmen durchzuführen.

Kontaktpersonen

1. Weisungsberechtigte des Auftraggebers:

Name ***(Position)***	**Telefon** **E-Mail**

2. Weisungsempfänger des Auftragnehmers:

Zum Empfang von Weisungen betreffend die Auftragsverarbeitung sind auf Seiten des Auftragnehmers folgende Personen bzw. Personengruppen berechtigt:

Name	**E-Mail**	**Telefon**
Dennis Liemann	dennis.liemann@bms-consulting.de	0173-6085843
Jan-Marvin Beyer	jan-marvin.beyer@bms-consulting.de	0173-7105970
Christian Pietruschka	christian-pietruschka@bms-consulting.de	0176-23996644
Support	support@bankingguide.de	0211-87580780

18.2 Anlage 2 – Genehmigte (Sub)unternehmer

BMS Consulting GmbH
Fürstenwall 172
40217 Düsseldorf
Deutschland

Aufgaben des Subunternehmers:
Die BMS Consulting GmbH übernimmt die Konfigurations- und Individualisierungsaufgaben für die BankingGuide GmbH.

Eudemonia Solutions AG
Fürstenwall 172
40217 Düsseldorf

Aufgaben des (Sub)unternehmers:
Die Eudemonia Solutions AG ist für die technische Entwicklung der Softwarelösung zuständig. Bei Bedarf kann es notwendig werden, Entwickler im Rahmen der Erstkonfiguration bzw. zur Bearbeitung von Support-Anfragen hinzuzuziehen.

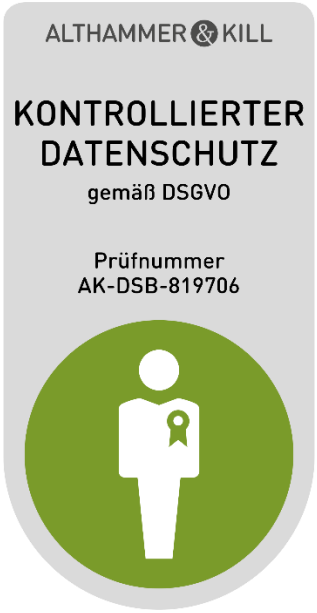
BMS Training und Coaching GmbH
Fürstenwall 172
40217 Düsseldorf
Deutschland

Aufgaben des Subunternehmers:
Die BMS Training und Coaching GmbH ist für die fachliche und methodische Qualifikation der Anwender verantwortlich. Nach Bedarf kann eine Unterweisung via Fernwartung erfolgen.

18.3 Anlage 3 - autorisierte Softwarelösungen

Software	Anbieter	Homepage
TeamViewer	TeamViewer GmbH Jahnstr. 30 73037 Göppingen	https://www.teamviewer.com/de/ Sicherheitsinformationen: https://dl.tvcdn.de/docs/de/TeamViewer-Security-Statement-de.pdf

18.4 Anlage 4 - Technische und organisatorische Maßnahme der BMS Berens Mosiek Siemes Consulting GmbH



Datenschutzbeauftragter: Niels Kill

Althammer & Kill GmbH & Co.KG
Neuer Zollhof 3
40221 Düsseldorf

T. +49 211 936748-20
F. +49 211 936748-21
M. nk@althammer-kill.de

www.althammer-kill.de

ALTHAMMER & KILL

Kontrollierter Datenschutz

gemäß DSGVO

Die Althammer & Kill GmbH & Co. KG bescheinigt hiermit, dass

BMS Berens Mosiek Siemes Consulting GmbH
Bahnstraße 16
40212 Düsseldorf

den Datenschutz nach den Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) gestaltet. Es sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten umgesetzt.

Der Datenschutzbeauftragte ist weisungsfrei und wirkt auf die Einhaltung der EU-Datenschutz-Grundverordnung und einschlägiger Rechtsvorschriften hin.

Datenschutzbeauftragte/r **Niels Kill**
Prüfnummer **AK-DSB-819706**

Düsseldorf, den 25.05.2018

Niels Kill
Geschäftsführer

Thomas Althammer
Geschäftsführer

ALTHAMMER & KILL
KONTROLLIERTER DATENSCHUTZ
gemäß DSGVO
Prüfnummer AK-DSB-819706

Althammer & Kill
GmbH & Co. KG
Thielenplatz 3
30159 Hannover
www.althammer-kill.de


BMS
CONSULTING
BMS Berens Mosiek Siemes Consulting GmbH
technische und organisatorische Maßnahmen
nach Art. 32 DSGVO, § 64 BDSG-neu
Düsseldorf, 01.06.2018

Inhalt

BMS Berens Mosiek Siemes Consulting GmbH - TOMs

3

1. Zweck des Dokumentes

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen der DSGVO erfüllt werden.

Zudem fordern die Datenschutzgesetze des Bundes und der Länder, dass für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen sind, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind.

In den folgenden Abschnitten werden die technischen und organisatorische Maßnahmen nach Art. 32 Datenschutz-Grundverordnung (DSGVO) und § 64 Bundesdatenschutzgesetz (BDSG neu) der BMS Berens Mosiek Siemes Consulting GmbH beschrieben.

TOMs der BMS Consulting GmbH_V1.3.docx | Stand: 01.05.2018

2. Technische und organisatorische Maßnahmen

2.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1.1. Zutrittskontrolle (Räume und Gebäude)

Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

- Einbruchshemmende Türen, Serverräume ohne Fenster
- Verwendung von Sicherheitsschlüsseln
- Schlüsselvergabe nur an berechtigte Personen (Schlüsselregelung)
- Führung eines Schlüsselverzeichnisses
- Sorgfältige Auswahl von Reinigungspersonal und externen Dienstleistern
- Protokollierung von Besuchern, Begleitung durch eigene Mitarbeiter

2.1.2. Zugangskontrolle (IT-Systeme und Anwendungen)

Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Zugang zu Computern nur mit Hilfe gesicherter Authentifizierungsverfahren (Benutzerkonto/Passwort)
- Individuelle, geheime und komplexe Passwörter, regelmäßige Änderungen
  - Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
  - Das Kennwort muss mindestens 8 Zeichen lang sein.
  - Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten:
    - Großbuchstaben (A bis Z)
    - Kleinbuchstaben (a bis z)
    - Zahlen zur Basis 10 (0 bis 9)
  - Nicht alphabetische Zeichen (zum Beispiel !, $, #, %)
  - Die Komplexitätsvoraussetzungen werden erzwungen, wenn Kennwörter geändert oder erstellt werden.
  - Kontosperrungen erfolgen automatisch nach 5 Fehlversuchen
- Vermeidung der Wiederholung von Passwörtern für andere Dienste/Anwendungen
- Einsatz stets aktuell gehaltener Anti-Viren-Software (Server und Clients)
- Remote-Zugänge durch verschlüsselte VPN-Tunnel mit zentraler Anmeldung
- Absicherung der DV-Systeme und Netzwerke gegen Zugänge von außen mittels Firewall
- Daten werden nur verschlüsselt in externen Backup-Systemen gelagert
- Verschlüsselung von mobilen Datenträgern
- Automatische Sperrung des Bildschirms
- Prozesse für Rechtevergabe/-entzug bei Eintritt, Veränderung und Austritt von Mitarbeitern
- Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- Verpflichtung aller Mitarbeiter auf Vertraulichkeit
- Protokollierung und Auswertung von Systemprotokollen

BMS Berens Mosiek Siemes Consulting GmbH - TOMs

2.1.3. Zugriffskontrolle (auf Daten und Informationen)

Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten Zugang haben und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Einsatz einer zentralen Firewall
- Berechtigungskonzept und individuelle Vergabe von Benutzerrechten (Rollen-basiert)
- Erteilung und Nutzung von Administratorenrechten auf das Notwendigste begrenzt (Trennung von User- und Admin-Accounts)
- Festlegung der Zugriffsberechtigung und der Befugnis zur Dateneingabe, -änderung, -löschung
- Trennung der Berechtigungsbewilligung (organisatorisch) und Vergabe (technisch)
- Regelmäßige Überprüfung der Zugriffsberechtigung
- Auswertung von Zugriffsprotokollen
- Konzept zur Laufwerksnutzung und –Zuordnung
- Datenschutzkonforme Vernichtung von Datenträgern und vertraulichen Unterlagen (Shredder der Sicherheitsstufe 4, Verwendung von „Datentonnen“)

2.1.4. Trennungskontrolle

Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Trennung von Speicherbereichen nach Kunden/Mandanten und Projekten
- Trennung von Zugriffen auf Basis von Organisations-/Abteilungs-/Teamgrenzen
- Separierung von Dateien bei Datenbanken
- Logische Trennung von Datenbeständen
- Trennung von Entwicklungs-, Test- und Produktivsystemen

2.1.5. Pseudonymisierung (Artikel 32 Abs. 1 lit. a DSGVO; Artikel 25 Abs. 1 DSGVO)

Maßnahmen die gewährleisten, dass bei der Verarbeitung personenbezogener Daten in einer Weise, die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

- Verwendung von Pseudonymisierungs- und Anonymisierungsverfahren sofern verfahrenstechnisch sinnvoll. In diesen Fällen erfolgt die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.
- Weitergabe von Daten nur in anonymisierter oder pseudonymisierter Form.

2.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.2.1. Weitergabekontrolle

Maßnahmen die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Einsatz der Systeme nur im privaten Netzwerk oder über verschlüsselte Verbindungen in öffentlichen Netzwerken (VPN-Tunnel)
- Für einen Zugriff auf die DV-Systeme muss sich ein Benutzer mittels Benutzernamen und Passwort authentifizieren.
- E-Mail-Richtlinie bzw. kein Versand personenbezogener Daten per E-Mail
- E-Mailversand erfolgt mittels TLS-Verschlüsselung (TLS 1.2)
- Einsatz von E-Mail-Signaturen
- Keine Einsicht auf Bildschirme von außerhalb des Gebäudes möglich
- Sorgfältige Auswahl von Transportpersonal-/Fahrzeugen bzw. sichere Verpackungen

2.2.2. Eingabekontrolle

Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Organisatorische Festlegung der Zuständigkeiten für die Eingabe (mittels Zugriffsrechte
- Veränderungen/Löschungen von personenbezogenen Daten durch den Auftragnehmer erfolgen ausschließlich nach Beauftragung durch den Auftraggeber.
- Protokollierung von Eingaben/Änderungen/Löschungen
- Protokollauswertung und Sicherung mehrere Versionssätze im Rahmen des Backups
- Kontrolle der Dateneingabe

2.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.3.1. Verfügbarkeitskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Einsatz von Rauchmelder und Feuerlöschern
- Nutzung von Systemen zum Schutz vor Blitzschäden und Spannungsschwankungen
- Klimatisierung und Überwachung von Temperatur und Feuchtigkeit an zentralen Systemen
- Einsatz von Firewall, Virenscanner, Spam-Filter,
- Regelmäßige Produkt-/Software-Updates
- Regelmäßige Untersuchung von Hard- und Software-Schwachstellen
- Notfallkonzept und Notfallplan
    - Regelmäßige Datensicherungen
    - getrennte Aufbewahrung der Sicherungen
    - Einsatz von unterbrechungsfreien Stromversorgungen (USV) an zentralen Komponenten

2.3.2. Wiederherstellbarkeit

Maßnahmen die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Spiegelung von Festplatten und Systemen
- Redundante Sicherung von Daten und Systemen
- Auslagerung von verschlüsselten Sicherungskopien
- Regelmäßige Überprüfung der Wiederherstellbarkeit
- Vertretungsregelungen für abwesende Mitarbeiter

2.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

2.4.1. Datenschutz-Management (Leitlinie(n), Richtlinien, Arbeitsanweisungen und Sicherheitskonzepte)

Datenschutzfreundliche Voreinstellung (Art. 25 DSGVO)

- Berücksichtigung der Datenschutzgrundsätze bei der Verarbeitung personenbezogener Daten
- Verarbeitung personenbezogener Daten nur für den bestimmten Verarbeitungszweck
- Regelmäßige Sensibilisierung (Infoveranstaltungen, Newsletter, Schulungen) der Mitarbeiter für das Thema Datenschutz
    - Schaffung eines Bewusstseins für eine sorgsame Absicherung des Arbeitsumfeldes.
    - Passworteingaben müssen unbeobachtet erfolgen,
    - geschäftliche Passwörter dürfen nicht außerhalb (z. B. privat zuhause) verwendet werden.

Kontrolle der Unterauftragnehmer

- Sorgfältige Auswahl geeigneter Dienstleister aufgrund von Standort und Datenschutz-Maßnahmen (Vorabüberzeugungspflicht)
- Zentrale Erfassung vorhandener Dienstleister
- Regelmäßige Überprüfung auf Eignung der Dienstleister
- Abschluss von Verträgen zur Auftragsdatenverarbeitung
- Schriftliche Weisungen und Festlegung der Zuständigkeiten, Kontrollrechte vereinbart
- Sichtung vorhandener IT-Sicherheitszertifikate und laufende Kontrolle der Auftragnehmer

BMS Berens Mosiek Siemes Consulting GmbH - TOMs

8

Regelmäßige Kontrollen, Dokumentation und ggf. Optimierung

- Es finden regelmäßige Kontrollen der Verarbeitungsverfahren statt. Basierend auf dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten, werden entsprechende Maßnahmen ergriffen, um den Datenschutzgrundsätzen - wie etwa Datenminimierung – gerecht zu werden
- Regelmäßige interne Kontrolle der getroffenen Sicherungsmaßnahmen. (ggf. Anpassung an den Stand der Technik)
- Prüfungen des externen Datenschutzbeauftragten auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme

TOMs der BMS Consulting GmbH_V1.3.docx | Stand: 01.05.2018