BankingGuide GmbH

Lizenzvertrag / Nutzungsbedingungen

zur Nutzung der Anwendung „BankingGuide ZV“

im Rahmen von ProFi ZV

Inhalt

1. Vertragsgegenstand ... 3
2. Nutzungsumfang ... 3
3. Wartung & Support ... 3
4. Vergütung ... 4
5. Gewährleistung ... 5
6. Erlaubnisse ... 5
7. Standort / Ort der Datenspeicherung ... 5
8. Dienstleistungsgüte ... 5
9. Steuerung und Kontrolle des ausgelagerten Bereiches ... 6
10. Rechte der Bankaufsicht ... 6
11. Bankgeheimnis / Geschäftsgeheimnis ... 6
12. Sonstige Informations- und Berichtspflichten ... 6
13. Fortwirkung von Rechten und Pflichten ... 7
14. Vertretungsregelung bei zentraler Auslagerungssteuerung ... 7
15. Sicherstellung Daten ... 7
16. IKT-bezogener Vorfall ... 8
17. Teilnahme an Schulungen ... 8
18. Haftung ... 8
19. Beendigung des Vertrages ... 8
20. Schlussbestimmungen ... 9
Anlage Subdienstleister ... 10
Anlage Informationssicherheit ... 11

1. Vertragsgegenstand

1. Gegenstand dieses Lizenzvertrags ist die Anwendung BankingGuide ZV im Rahmen von ProFi ZV und dessen optionale Erweiterungskomponenten (im Folgenden "Software BankingGuide" genannt).

2. Die BankingGuide GmbH räumt der Bank das Recht ein, die von der Banking-Guide GmbH entwickelte Software BankingGuide sowie den darin enthaltenen Master-Content zu diesen Vertragsbedingungen zu nutzen. Über den Master-Content hinausgehende Inhalte sowie sonstige Medien und Inhalte sind durch die Bank bereitzustellen.

2. Nutzungsumfang

1. Die Bank erhält das nicht ausschließliche, auf die Dauer des Vertragsverhältnisses zeitlich begrenzte Recht, die Software BankingGuide in der ihm gelieferten Version im eigenen Betrieb zu nutzen. Das Nutzungsrecht gilt für eine unbegrenzte Anzahl von gleichzeitigen Zugriffen, d.h. für eine unbegrenzte Anzahl von Clients, die gleichzeitig mit der Software BankingGuide arbeiten.

2. Die Software BankingGuide wird auf der Omnikanalplattform der Atruvia AG betrieben. Die Software BankingGuide wird ausschließlich über die Omnikanalplattform der Atruvia AG in Verbindung mit der Anwendung „KBM FK - Kundenbeziehungsmanagement Firmenkunden“ aufrufbar und benutzbar sein. Die Schaffung der technisch-organisatorischen Rahmenbedingungen zur Nutzung der Omnikanalplattform obliegt der Bank. Die Nutzung der Software BankingGuide umfasst neben der Nutzung der Beratungsanwendung auch den Zugriff auf die Administration der Software.

3. Die Bank wird die in der Software BankingGuide angebrachten Copyright-Vermerke und -Kennzeichen beachten.

4. Die Bank verpflichtet sich, die Software BankingGuide und die betreffenden Inhalte (Content), Handbücher und Dokumentationen Dritten weder ganz noch teilweise zugänglich zu machen. Entsprechende Geheimhaltungspflichten sind auch den mit diesem Lizenzmaterial in Kontakt kommenden Mitarbeitern aufzuerlegen. Unterlizenzen kann die Bank nicht erteilen. Eine Übertragung der Lizenz auf Dritte ist nur zusammen mit einer Veräußerung des ganzen Betriebs und nur unter der weiteren Voraussetzung zulässig, dass der Erwerber sich gegenüber der BankingGuide GmbH schriftlich in der gleichen Weise wie zuvor die Bank zum Schutz des Lizenzmaterials verpflichtet.

3. Wartung & Support

1. Im Rahmen der Softwarewartung stehen der Bank die nachfolgenden Dienstleistungen der BankingGuide GmbH zur Verfügung:

a. 1st- und 2nd-Level-Support
   Die BankingGuide GmbH nimmt die gemeldeten Probleme mit der Software BankingGuide unter dem Support-Ticketsystem der Omnikanalplattform (ITSM) (Prio 1) sowie der Mailadresse support@bankingguide.de (Prio 2) entgegen und bearbeitet diese zeitnah.

b. Softwareinformationen
   Die BankingGuide GmbH wird die Bank durch die Herausgabe von Informationen über bevorstehende Updates und Produktreleases sowie Anwendungstechniken und Problemlösungen regelmäßig informieren.

c. Lieferung von Korrekturversionen
   Die BankingGuide GmbH wird die der Bank überlassene Software BankingGuide inklusive der Dokumentationen in unregelmäßigen Abständen überarbeiten und entsprechende Softwareergänzungs- oder - korrekturlieferungen herausbringen.

2. Hiervon unberührt bleiben zukünftig neu entwickelte Softwarekomponenten. Die Lieferung neuer Programmversionen oder neu entwickelter Komponenten ist nicht Bestandteil der Wartungsleistungen und wird der Bank zu einer entsprechenden Lizenzgebühr gesondert angeboten.

4. Vergütung

1. Die Vergütung setzt sich aus mehreren Preiskomponenten zusammen. Die Zusammensetzung und Höhe der Vergütung sind den jeweiligen Bestellformularen zur Software BankingGuide zu entnehmen.

2. Bei der Ermittlung des variablen Nutzungsentgelts wird auf die Höhe der Bilanzsumme des Lizenznehmers abgestellt. Zur Ermittlung der Höhe der Bilanzsumme des Lizenznehmers wird der letzte testierte Jahresabschluss herangezogen. Dieser muss vom Lizenznehmer an die BankingGuide GmbH übermittelt und bei Änderungen innerhalb einer angemessenen Frist aktualisiert werden.

3. Die Rechnungsstellung für die Software BankingGuide erfolgt durch die BankingGuide GmbH jeweils zum Beginn eines Kalenderjahres. Bei unterjährigen Bestellungen wird im ersten Jahr die anteilige Jahresgebühr (volle Restmonate) berechnet.

4. Bei Zahlungsverzug berechnet die BankingGuide GmbH der Bank Verzugszinsen in der jeweils gesetzlich festgelegten Höhe.

5. Alle Beträge verstehen sich zzgl. der gesetzlichen Mehrwertsteuer.

5. Gewährleistung

1. Die BankingGuide GmbH steht dafür ein, dass die Software BankingGuide die Funktionen der Leistungsbeschreibung erfüllt und nicht mit Fehlern behaftet ist, die den Wert oder die Tauglichkeit zu dem gewöhnlichen oder nach dem Vertrag vorausgesetzten Gebrauch aufheben oder mindern.

2. Die Gewährleistungsfrist der BankingGuide GmbH beträgt 12 Monate und beginnt am Tag der Auslieferung der Software BankingGuide an die Bank.

3. Gegenstand der Gewährleistung ist die Software BankingGuide ausschließlich in der von der BankingGuide GmbH ausgelieferten Version. Fehler an der Software, die auf nachträgliche Eingriffe des Lizenznehmers zurückzuführen sind, sind nicht Gegenstand der Gewährleistung.

4. Mängel hat die Bank der BankingGuide GmbH unverzüglich anzuzeigen. Die Anzeige hat schriftlich zu erfolgen. Ihr ist soweit möglich eine nachvollziehbare Beschrei-bung des Mangels beizufügen.

5. Erlaubnisse

Der Auftragnehmer verfügt über etwaig für die (IKT- und/oder sonstige) mit diesem Vertrag übernommene Leistungserbringung (in diesem Vertrag „ausgelagerte Aktivitäten und Prozesse“ oder „Auslagerungstätigkeit“ genannt) erforderlichen Erlaubnisse und Registrierungen. Soweit zukünftig Erlaubnisse und Registrierungen erforderlich werden, verpflichtet er sich, diese umgehend einzuholen.

6. Standort / Ort der Datenspeicherung

Der Standort der Durchführung der Dienstleistung und Standort der Speicherung sowie Verarbeitung maßgeblicher Daten durch den Auftragnehmer oder ggf. (z.B. aufgrund Weiterverlagerung eingeschaltete) Dritte werden in der Anlage 1 zum Vertrag abgebildet. Über den Wechsel des jeweiligen Standorts ist die Bank mittels Aktualisierung der vorgenannten Anlage rechtzeitig vorab zu informieren.

7. Dienstleistungsgüte

Der Auftragnehmer verpflichtet sich, bei Erbringung der Auslagerungstätigkeit die diesbezüglich jeweils gesetzlich oder sonst für die Bank zwingend vorgegebenen Standards (einschließlich Datenschutz und Bankgeheimnis) einzuhalten, auch wenn diese über die konkret vereinbarten Standards hinausgehen. Er gewährleistet, dass er seine Dienstleistung in einer Form erbringt, die es der Bank ermöglicht, den ihr obliegenden Pflichten gegenüber Kunden und Aufsichtsbehörden zu entsprechen. Weitere Standardveränderungen/ -verbesserungen unterliegen einer einvernehmlichen Absprache zwischen den Vertragsparteien.

8. Steuerung und Kontrolle des ausgelagerten Bereiches

Die Bank ist gesetzlich verpflichtet, ausgelagerte Aktivitäten und Prozesse (Betriebsbereiche) in ihre internen Kontrollverfahren einzubeziehen, um die Ordnungsmäßigkeit der diesbezüglichen Geschäftsführung und die Beibehaltung der Steuerungs- und Kontrollmöglichkeiten der Geschäftsleitung gewährleisten zu können (§ 25b KWG bzw. Art. 5 der Verordnung (EU) 2022/2554 („DORA“)). Außerdem dürfen Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der zuständigen Bankaufsichts- oder Abwicklungsbehörden nicht durch die Auslagerung beeinträchtigt werden.

9. Rechte der Bankaufsicht

Der Auftragnehmer erklärt sich bereit, soweit dies gesetzlich zulässig ist, etwaige Informations- und Prüfungsmaßnahmen der zuständigen Bankaufsichts- und Abwicklungsbehörden sowie von dieser mit der Prüfung beauftragten Stellen bzw. benannten Personen bezüglich der Auslagerungstätigkeit uneingeschränkt zu dulden und mit diesen im Rahmen der Wahrnehmung ihrer behördlichen Aufgaben vollumfänglich zusammenzuarbeiten.

10. Bankgeheimnis / Geschäftsgeheimnis

Der Auftragnehmer ist zeitlich unbegrenzt gemäß den allgemein gültigen Regelungen in Bezug auf Geschäftsgeheimnisse und entsprechend der für die Bank geltenden Pflicht zur Einhaltung des Bankgeheimnisses zur Verschwiegenheit über die Geschäftsgeheimnisse der Bank, die Umstände der Auslagerung sowie die dabei erlangten Daten und sonstigen Informationen verpflichtet. Insbesondere ist er zur Verschwiegenheit über alle auf die Kunden der Bank bezogenen Tatsachen und Wertungen verpflichtet, von denen er Kenntnis erlangt. Er verpflichtet sich, die Vertraulichkeit der Kundendaten nicht nur gegenüber Dritten, sondern durch besondere technische, personelle und organisatorische Maßnahmen auch im Verhältnis zwischen verschiedenen Banken zu wahren. Informationen über Kunden der Bank darf er nur dann weitergeben, wenn gesetzliche Bestimmungen dies gebieten oder die Bank ihn mit der Weitergabe der Daten beauftragt hat.

Sofern die Auslagerungstätigkeit die Verarbeitung von Daten natürlicher Personen betrifft, bleiben im Übrigen die diesbezüglich einschlägigen datenschutzrechtlichen Bestimmungen nebst etwaigen ergänzenden Vereinbarungen zwischen Bank und Auftragnehmer unberührt.

11. Sonstige Informations- und Berichtspflichten

Der Auftragnehmer verpflichtet sich, der Bank die zur aufsichtsrechtlich (insbesondere nach Maßgabe der Mindestanforderungen an das Risikomanagement – MaRisk – der BaFin bzw. – sofern relevant – der DORA in ihrer jeweiligen Fassung) vorgegebenen Führung eines Auslagerungs- bzw. Informationsregisters benötigte Angaben zur Verfügung zu stellen und diesbezügliche Änderungen unverzüglich der Bank zu übermitteln.

12. Fortwirkung von Rechten und Pflichten

Die nach Nr. 9 (Steuerung und Kontrolle des ausgelagerten Bereiches) + Nr. 10 (Rechte der Bankaufsicht) dieses Vertrages vereinbarten Rechte und Pflichten bestehen noch für die Dauer von 2 Geschäftsjahren nach Ablauf des Geschäftsjahres fort, in dem der Vertrag – sei es durch Kündigung oder aus anderem Grund – im Übrigen seine Gültigkeit verliert. Geschäftsjahr im Sinne vorstehender Regelung ist das Geschäftsjahr der Bank.

Soweit bei der Bank für alle oder Teile von Unterlagen bezüglich der ausgelagerten Aktivitäten und Prozesse eine gesetzliche Aufbewahrungspflicht besteht (z.B. nach § 257 HGB, § 25a Abs. 1 KWG, § 147 AO), verpflichtet sich der Auftragnehmer zur Aufbewahrung dieser Unterlagen entsprechend dieser Pflichten bzw. – auf Verlangen der Bank– zur Herausgabe dieser Unterlagen, jeweils auch nachdem der Vertrag im Übrigen seine Gültigkeit verliert. Hierfür teilt die Bank dem Auftragnehmer diejenigen gesetzlichen Aufbewahrungsfristen mit, die für sie einschlägig sind. Der Auftragnehmer wird der Bank im Bedarfsfalle das uneingeschränkte Eigentum an den Unterlagen verschaffen.

13. Vertretungsregelung bei zentraler Auslagerungssteuerung

Der Auftragnehmer erklärt sich bereit und ist hierzu berechtigt, Informationen und Erklärungen, die er der Bank gegenüber auf Grund der Vorgaben der MaRisk oder DORA abzugeben bzw. an diese zu übermitteln hat, gegenüber dem zentralem Auslagerungsmanagementunternehmen abzugeben. Entsprechendes gilt entsprechend für eingeräumte Prüfungs- und Kontrollrechte, deren Geltendmachung die Bank an das zentrale Auslagerungsmanagementunternehmen übertragen hat. Dieses setzt voraus, dass das zentrale Auslagerungsunternehmen eine mindestens in Textform abgefasste Ermächtigung der Bank hierzu vorlegen kann.

14. Sicherstellung Daten

Der Auftragnehmer einer IKT-Dienstleistung ist verpflichtet, im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit oder einer Beendigung, der Bank Zugang zu den zu diesem Zeitpunkt beim Auftragnehmer vertragsgemäß zu speichernden personenbezogenen und nicht personenbezogen Daten der Bank zu gewähren, diese auf Anforderung unverzüglich wiederherzustellen und zurückzugeben, sofern rechtlich zulässig. Diese Rückgabe hat in einem leicht zugänglichen Format in, sofern nicht anderweitig vereinbart, elektronischer Form an die Bank oder an einen von der Bank benannten Dritten zu erfolgen. Auf Verlangen der Bank hat der Auftragnehmer sämtliche verbliebenen Datenbestände der Bank unwiderruflich zu löschen.

Sofern die Möglichkeit besteht, dass die Zugriffsmöglichkeit der Bank auf ihre Daten beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet wird oder absehbar gefährdet werden könnte, so hat der Auftragnehmer die Bank unverzüglich zu verständigen und alles seinerseits Erforderliche zu tun, um die Zugriffsmöglichkeit der Bank sicherzustellen.

15. IKT-bezogener Vorfall

Der Auftragnehmer ist verpflichtet, der Bank bei einem IKT-bezogenen Vorfall i.S.d. Art 3 Nr. 8 DORA, der mit der bereitgestellten Leistung in Verbindung steht, Unterstützung zu leisten. Details hierzu sind in der Anlage Informationssicherheit geregelt.

Der Auftragnehmer wird für die Mitwirkung eine für die vertragliche Hauptleistung entsprechende Vergütung erhalten. Der Auftragnehmer hat jedoch den ihm entstandenen Aufwand nachzuweisen.

16. Teilnahme an Schulungen

Der Auftragnehmer verpflichtet sich, seine Mitarbeiter, die Geschäftsleitung und ggf. eingesetzte Unterauftragnehmer (im Folgenden „eingesetzte Mitarbeiter“) auf Basis eines Schulungs- und Sensibilisierungskonzeptes entsprechend Ihrer Aufgaben und Verantwortung regelmäßig zu Aspekten der Informationssicherheit zu schulen und zu sensibilisieren. Die Inhalte der Schulungs- und Sensibilisierungsmaßnahmen sowie der Teilnahme der eingesetzten Mitarbeiter als auch das zugrunde liegende Schulungs- und Sensibilisierungskonzept werden der Bank auf Anfrage in qualifizierter Form glaubhaft gemacht oder in sonstiger Form angemessen nachgewiesen.

Sollen darüber hinaus Schulungs- und Sensibilisierungsmaßnahmen bei der Bank für bei der Bank eingesetzte Mitarbeiter erfolgen, werden die Parteien sich über einen angemessenen Umfang und die Kostentragung einigen.

17. Haftung

1. Die BankingGuide GmbH haftet uneingeschränkt nur für Vorsatz und grobe Fahrlässigkeit der BankingGuide GmbH, ihrer gesetzlichen Vertreter oder Erfüllungsgehilfen sowie für Schäden aus Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer Pflichtverletzung beruhen, die die BankingGuide GmbH, ihre gesetzlichen Vertreter oder Erfüllungsgehilfen zu vertreten haben.
2. Sofern die BankingGuide GmbH oder ein gesetzlicher Vertreter oder Erfüllungsgehilfe schuldhaft eine wesentliche Vertragspflicht („Kardinalpflicht“) verletzt, ist die Haftung auf den vertragstypischen, vorhersehbaren Schaden begrenzt; im Übrigen ist sie ausgeschlossen.
3. Die BankingGuide GmbH haftet nicht für Schäden, sofern oder soweit die Bank deren Eintritt durch ihm zumutbare Maßnahmen hätte verhindern können.
4. Die Bestimmungen des Produkthaftungsgesetzes bleiben unberührt.

18. Beendigung des Vertrages

Mit einer Kündigungsfrist von 12 Monaten kann die Nutzung des Softwareprodukts BankingGuide oder einer optionalen Erweiterungskomponente zum Ende eines Kalenderjahres von beiden Vertragsparteien beendet werden. Die Kündigung bedarf der Schriftform und ist an die

BankingGuide GmbH (bei Kündigung durch die Bank) oder an die juristische Adresse der Bank (bei Kündigung durch die BankingGuide GmbH) zu richten.

Nach erfolgter Kündigung wird der Benutzerzugang durch die BankingGuide GmbH zum Kündigungszeitpunkt gesperrt.

Der Vertrag kann von beiden Seiten außerordentlich gekündigt werden, wenn ein Abwarten bis zur ordnungsgemäßen Vertragsbeendigung nach § 5 Abs. 1 dieses Vertrages der kündigenden Partei nicht zumutbar ist. Die außerordentliche Kündigung ist spätestens drei Monate nach dem Zeitpunkt zu erklären, zu welchem die verletzte Partei von dem Vertragsverstoß erfahren hat.

Unbeschadet sonstiger Kündigungsregelungen im Vertrag hat die Bank in nachfolgenden Fällen ein außerordentliches Kündigungsrecht:

1. es liegt ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen vor;
2. es liegen Umstände vor, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des Auftragnehmers auswirken;
3. es liegen nachweisliche Schlechtleistungen des Auftragnehmers in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, vor, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt;
4. die zuständige Behörde kann die Bank infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen.

19. Schlussbestimmungen

1. In dieser Vereinbarung sind sämtliche Rechte und Pflichten der Vertragsparteien geregelt. Änderungen oder Ergänzungen bedürfen der Schriftform.

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. Dieser Vertrag unterliegt ausschließlich deutschem Recht. Die Anwendung des UN-Kaufrechts (CISG) wird ausdrücklich ausgeschlossen. Ausschließlicher Gerichtsstand für beide Seiten ist Düsseldorf.

Anlage Subdienstleister

Subdienstleister	Standort der Leistungserbringung / Datenverarbeitung
BMS Corporate Solutions GmbH	Fürstenwall 172 40217 Düsseldorf

Anlage Informationssicherheit

1. Geltungsbereich der Anforderungen

Die im Folgenden beschriebenen Anforderungen beziehen sich ausschließlich auf die von Seiten des Auftragnehmers zu erbringenden vertraglichen Leistungen gemäß der Leistungsbeschreibung des Hauptvertrags. Die Anforderungen an die Informationssicherheit betreffen somit alle Mitarbeiter, Systeme der Informations- und Kommunikationstechnologie (IKT-Systeme) und Einrichtungen des Auftragnehmers, die in eine Verarbeitung der Informationen der Bank involviert sind.

Die Anforderungen gelten risikoorientiert auch für Dritte („Unterauftragnehmer“), die der Auftragnehmer mit von ihm zu erbringenden Leistungen nach Maßgabe der Nr. 9 Steuerung und Kontrolle des ausgelagerten Bereiches beauftragt. Der Auftragnehmer hat die Anforderungen gegenüber seinen Unterauftragnehmern vertraglich sicherzustellen.

2. Informationssicherheitsmanagement

Der Auftragnehmer ist verpflichtet, die von ihm gegenüber der Bank zu erbringenden Leistungen in sein Informationssicherheitsmanagement einzubeziehen. Im Rahmen seines Informationssicherheitsmanagements trifft der Auftragnehmer unter anderem geeignete technische und organisatorische Maßnahmen, um ein dem Risiko für die Informationssicherheit sowie in Bezug auf die Schutzziele Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten und Informationen der Bank angemessenes Schutzniveau - wie in den folgenden Absätzen weiter ausgeführt - zu erreichen und zu wahren. Zudem sind die Eintrittswahrscheinlichkeit und die Schwere eines aus einer möglichen Verletzung der Informationssicherheit resultierenden Risikos, sowie der Stand der Technik, angemessene Standards für Informationssicherheit [z.B. IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der internationale Sicherheitsstandard ISO/IEC 2700X der International Organisation for Standardization] zu berücksichtigen. Dies beinhaltet auch Maßnahmen, die darauf ausgerichtet sind, Cyberrisken angemessen zu steuern.

Der Auftragnehmer ist dazu verpflichtet, Maßnahmen, Tools, Leit- und Richtlinien für Informationssicherheit vorzuhalten, die ein angemessenes Maß an Sicherheit für die Erbringung der IKT-Dienstleistungen durch die Bank bieten.

Änderungen seiner von dem Auftragnehmer zu beachtenden Sollvorgaben zur Informationssicherheit teilt die Bank dem Auftragnehmer mit einem Vorlauf von mindestens 12 Wochen mit.

3. Weiterentwicklung des Informationssicherheitsmanagements

Der Auftragnehmer wird die Maßnahmen unter Berücksichtigung des technischen Fortschritts und dem Bekanntwerden neuer Risiken für die Informationssicherheit stetig weiterentwickeln. Wesentliche Änderungen der Maßnahmen, die Einfluss auf die Integrität, Vertraulichkeit, Authentizität oder Verfügbarkeit, der im Kontext der Leistungserbringungen betroffenen Daten

und Informationen haben können, wird der Auftragnehmer der Bank mitteilen, wobei die Bank solchen Änderungen nur aus wichtigem Grund widersprechen kann. Als wichtiger Grund gilt insbesondere, wenn begründeter Anlass zu Zweifeln bezüglich des ordnungsgemäßen Schutzes der Informationen der Bank besteht. Die Bank kann jederzeit eine aktuelle Beschreibung der vom Auftragnehmer konkret getroffenen technischen und organisatorischen Maßnahmen anfordern.

4. Pflichten zur Information bei und Behandlung von Informationssicherheitsverletzungen

Der Auftragnehmer hat Unregelmäßigkeiten in der Verarbeitung von Informationen, sowie alle sicherheitsrelevanten Vorfälle, die zu einer Verletzung mindestens eines der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität führen (nachfolgend gemeinsam „IKT-bezogener Vorfall“), wie ein nicht geplantes oder unerwartetes Ereignis oder eine Reihe solcher Ereignisse, die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigen und die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten der Bank unmittelbar oder mittelbar zu gefährden und die Informationssicherheit zu bedrohen, unverzüglich (ohne schuldhaftes Zögern) nach Bekanntwerden zu melden und zu dokumentieren. Der Auftragnehmer hat zur Erkennung und Behandlung von IKT-bezogenen Vorfällen angemessene Systeme, Prozesse und Verantwortlichkeiten implementiert. Dabei sind die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu berücksichtigen.

Der Auftragnehmer unterstützt die Bank und die zuständigen Behörden bei der Erfüllung der ihr bei einem schwerwiegenden IKT-bezogenen Vorfall obliegenden Pflichten und erteilt ihr die in diesem Zusammenhang erforderlichen weiteren Informationen.

Die Dokumentation und Meldung eines IKT-bezogenen Vorfalls enthalten mindestens folgende Informationen:

1. eine Beschreibung der Art des IKT-bezogenen Vorfalls, der betroffenen Informationen, der voraussichtlichen Folgen und der von dem Auftragnehmer ergriffenen oder beabsichtigten Maßnahmen zur Behebung des Informationssicherheitsvorfalls und der nachteiligen Auswirkungen
2. Informationen aus der Fehler- bzw. Ursachenanalyse
3. falls zutreffend den durchgeführten Notfallvorsorgemaßnahmen
4. den Namen und die Kontaktdaten des Informationssicherheitsbeauftragten oder eines anderen Ansprechpartners.

Der Auftragnehmer hat zur Erkennung und dem Management von Schwachstellen angemessene Systeme, Prozesse und Verantwortlichkeiten zu implementieren. Der Auftragnehmer hat kritische Schwachstellen zeitnah zu melden.

5. Ermöglichung von uneingeschränkten Kontrollen

In den Fällen, in welchen die Bank nach dem Hauptvertrag (bzw. ihrer AGB oder Anlagen) das Recht hat bei Unterstützung kritischer oder wichtiger Funktionen, eigene Prüfungen durch ihre Interne Revision oder durch einen von dieser bestellten Prüfer beim Auftragnehmer durchzuführen, zählen zu den etwaig bestellten Prüfern auch das

Informationssicherheitsmanagement der Bank oder deren Beauftragter bzw. externe Informationssicherheitsprüfer der Bank.

6. Kommunikation

Der Auftragnehmer richtet Informationen, Meldungen und Fragen zur Informationssicherheit an diejenige Kontaktperson, die ihr innerhalb von 14 Tagen nach Abschluss dieses Vertrages von der Bank an kontakt@bankingguide.de mitgeteilt wurde.

Der Auftragnehmer nennt der Bank einen zentralen Ansprechpartner (inklusive der aktuellen Kontaktdaten), der im Unternehmen des Auftragnehmers im Auftrag der Leitungsebene die Aufgabe Informationssicherheit koordiniert, innerhalb des Unternehmens vorantreibt und als Ansprechpartner verantwortet. Die Bank kann sich jederzeit mit Fragen zur Informationssicherheit an isb@bms-cs.de wenden.