banking & network it solutions GmbH

Klosterdorf 38, 91443 Scheinfeld
Telefon: +49 9162 - 5279990
Telefax: +49 9162 - 5279998
E-Mail: info@bn-its.de, Internet: http://www.bn-its.de

Auslagerungsvereinbarung der bn-its banking & network it solutions GmbH

1 Vertragsgegenstand

Voraussetzung für die nachfolgend aufgeführten Vertragspunkte ist eine aktive „Compliance Pauschale“ (zu den jeweils aktuellen Konditionen). Bei Kündigung oder Erreichen des Laufzeitende der „Compliance-Pauschale“ erlöschen die gewährten Rechte.

1.1 Dienstleistungsgüte und Service Level

Eine detaillierte Beschreibung der Dienstleistungsgüte gemäß Art. 30 Abs. 2 lit. e) DORA sowie die ggf. geltenden Service Level sind in den jeweiligen Verträgen und Produktartikeln der einzelnen Leistungen definiert.
Die aktuellen Support-Zeiten sind jederzeit auf der Website von bn-its abrufbar.

1.2 Geltendes Recht

Dieser Vertrag unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland und wird auf Basis deutscher Gesetze und Rechtsprechung der deutschen Gerichtsbarkeit sowie des Europäischen Gerichtshofs ausgelegt.
Der Auftragnehmer versichert, dass er über alle erforderlichen Erlaubnisse, Registrierungen und Zulassungen für die Erbringung der vertraglich vereinbarten Leistungen verfügt. Sollten zukünftig weitere behördliche Genehmigungen oder Registrierungen erforderlich werden, verpflichtet sich der Auftragnehmer, diese unverzüglich und fristgerecht einzuholen.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen bereitzustellen, die zur Erfüllung gesetzlicher Pflichten erforderlich sind. Dies umfasst insbesondere die Bereitstellung von Daten und Nachweisen für die Erstellung von Informationsregistern gemäß DORA sowie für das Auslagerungsregister nach MaRisk. Der Auftragnehmer wird sicherstellen, dass diese Informationen in einer geeigneten Form und innerhalb angemessener Fristen zur Verfügung gestellt werden, um die Einhaltung regulatorischer Anforderungen zu gewährleisten.

1.3 Standorte

Die Dienstleistung des Auftragnehmers wird in Deutschland erbracht. Es werden alle prozessrelevanten Daten und Informationen beim Auftraggeber gespeichert. Sofern notwendig werden die Daten, die für die Dienstleistung gespeichert werden, entsprechend den Vorgaben der DSGVO in Europa gespeichert. Sofern der Standort für die Leistungserbringung bzw. die Speicherung von Daten verlagert wird und damit die definierte Region verlässt, wird der Auftragnehmer den Auftraggeber benachrichtigen.

1.4 Überprüfung Notfallkonzepte

Der Auftragnehmer und die zu erbringende Dienstleistung sind nicht in die Prozesse und den IT-Betrieb des Auftraggebers eingebunden. Alle prozessrelevanten Daten werden beim Auftraggeber gespeichert. Es findet keine Datenverarbeitung durch den Auftragnehmer im Auftrag des Auftraggebers statt. Insofern sind eine Einbindung, Abstimmung und regelmäßige Überprüfung der

Notfallkonzepte für diese Auslagerung nicht relevant. Der Auftragnehmer stellt einen 3rd. Level-Support zur Verfügung. Für den 3rd. Level-Support und die Erreichbarkeit der Mitarbeiter verfügt der Auftragnehmer über ein Notfallkonzept. Die entsprechenden Kontaktdaten werden dem Auftraggeber zur Verfügung gestellt.

1.5 Informations- und Prüfungsrechte

Es werden Informations- und Prüfungsrechte für die Interne Revision sowie der Abschlussprüfer vereinbart. Im Rahmen der Informationsrechte wird der Auftragnehmer von einem Wirtschaftsprüfer erstellte Prüfungsberichte nach IDW PS 951 bzw. ähnlicher Standards über das dienstleistungsbezogene interne Kontrollsystem auf Kosten des Auftraggebers erstellen lassen. Sobald der Bericht vorliegt, wird dieser dem Auftraggeber zur Verfügung gestellt. Der internen Revision und dem Abschlussprüfer des Auftraggebers werden Prüfungsrechte in Bezug auf das dienstleistungsbezogene interne Kontrollsystem zugesichert. Dies umfasst auch entsprechende Zutritts-, Zugangs- oder Zugriffsrechte. Da die MaRisk den Verzicht auf eigene Revisionshandlungen ermöglicht, wird die Interne Revision des Auftraggebers, im Rahmen Ihrer Revisionstätigkeit, ergänzende Prüfungshandlungen erst dann wahrnehmen, wenn der Auftragnehmer seinen Informationspflichten nicht nachkommt bzw. aus den zur Verfügung gestellten Unterlagen und Informationen für den Auftraggeber Pflichtverletzungen nicht ausgeschlossen werden können. Nach Beendigung des Vertrages gilt das eingeräumte Prüfungsrecht für zwei Jahre weiter. Die im Rahmen der durch den Auftraggeber durchgeführten Prüfungen anfallenden Zeiten für Betreuung der Prüfer werden dem Auftraggeber mit dem zu dem Zeitpunkt der Prüfungen geltenden Stundensätzen in Rechnung gestellt.

Es dürfen durch diese Auslagerung die Prüfungsrechte sowie die Kontrollmöglichkeiten der gemäß §25b Absatz 3 KWG zuständigen Behörden bezüglich der ausgelagerten Aktivitäten und Prozesse nicht beeinträchtig werden. Daher wird der Auftragnehmer Prüfungen durch die zuständige Behörde dulden und entsprechende Zutritts-, Zugangs- und Zugriffsrechte gewähren, sofern Sie die ausgelagerte Dienstleistung bzw. das dienstleistungsbezogene interne Kontrollsystem betreffen. Die im Rahmen der durch die Aufsichtsbehörde durchgeführten Prüfungen anfallenden Zeiten für Betreuung der Prüfer werden dem Auftraggeber mit dem zu dem Zeitpunkt der Prüfungen geltenden Stundensätzen in Rechnung gestellt.

1.6 Weisungsrechte

Die zu erbringenden Dienstleistungen des Auftragnehmers werden in Service- und Support-Verträgen oder bei individueller Beauftragung separat geregelt, es werden hier keine weitergehenden Weisungsrechte des Auftragnehmers vereinbart.

1.7 Vertragsbeendigung

Der Auftragnehmer wird den Auftraggeber im Falle der Beendigung der vertraglichen Beziehung bei der Überleitung unterstützen. Die dazu aufgewendeten Zeiten und Kosten wird der Auftragnehmer dem Auftraggeber entsprechend der zum Zeitpunkt geltenden Stundensätze in Rechnung stellen. Es wird darauf hingewiesen, dass dem Auftraggeber grundsätzlich alle notwendigen Dokumentationen im Rahmen entsprechender Installations- und Konfigurationstätigkeiten zur Verfügung gestellt werden.

Der Auftraggeber hat nach Art. 28 Abs. 7 lit. A DORA ein Sonderkündigungsrecht in folgenden Fällen:

a) es liegt ein erheblicher Verstoß des Auftragnehmers gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen vor.

b) 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.

c) 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.

d) die zuständige Behörde kann den Auftraggeber infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen.

Der Auftraggeber stellt sicher, dass alle für die Erfüllung dieses Vertrages relevanten Daten in seinen eigenen Systemen gespeichert werden.

Sollten dennoch Daten beim Auftragnehmer gespeichert sein, verpflichtet sich dieser, dem Auftraggeber bei Vertragsbeendigung Zugang zu diesen Daten zu gewähren. Auf Verlangen des Auftraggebers müssen diese Daten entweder wiederhergestellt, zurückgegeben oder - sofern keine gesetzlichen oder regulatorischen Aufbewahrungspflichten bestehen - unverzüglich gelöscht werden.

1.8 Weiterverlagerung

Auf folgende Subdienstleister sind aktuell Teilprozesse verlagert:

- Zendesk (Ticketsystem)
- Firstcolo GmbH (IT-Rechenzentrum - Serverhousing)
- LANCOM (LMC - LANCOM Management Cloud)
- IONOS (IT-Rechenzentrum - Serverhousing)

Zendesk wird als Ticket-System vom Auftragnehmer genutzt. Darüber sind keine Teilprozesse des Auftraggebers abgebildet. Daher wird es nicht als Weiterverlagerung im Sinne der TZ 9 der MaRisk eingestuft. Zendesk stellt dem Auftragnehmer zur Erfüllung der Datenschutzrechtlichen Anforderungen die notwendigen Zertifizierungen (SOC2) bereit.

1.9 Informationspflichten

Der Auftragnehmer wird den Auftraggeber über Entwicklungen, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können, umgehend nach Kenntnisnahme informieren.

Der Auftragnehmer ist nicht in die Prozesse und den IT-Betrieb des Auftraggebers eingebunden. Der Auftragnehmer verfügt über keine eigene Interne Revision. Die Überwachungsfunktion im Sinne einer Internen Revision übernimmt beim Auftragnehmer die Geschäftsleitung sowie für ausgewählte Bereiche der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte.

1.10 Aufbewahrung

Der Auftragnehmer erstellt im Rahmen von Installations- und Konfigurationstätigkeiten Dokumentationen, die für den IT-Betrieb notwendig sind und stellt diese dem Auftraggeber zur Verfügung. Insofern liegt die Verantwortung für die Archivierung beim Auftraggeber. Da keine aufsichtsrechtlichen Prozesse auf den Auftragnehmer verlagert wurden, entfallen die sich aus dem KWG ergebenden Aufbewahrungspflichten für den Auftragnehmer. Die für die Dienstleistung erstellten Organisationsunterlagen (Kontrollbeschreibung) werden entsprechend AT 6 der MaRisk für 5 Jahre aufbewahrt.

1.11 Dokumentation

Vor dem Hintergrund, dass der Auftragnehmer jährlich eine Prüfung nach IDW PS 951 „Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“ von einem Wirtschaftsprüfer durchzuführen hat, muss der Auftragnehmer eine Kontrollbeschreibung des dienstleistungsbezogenen internen Kontrollsystems erstellen und diese aktuell halten. Diese gilt als schriftlich fixierte Ordnung im Sinne des KWG.

1.12 Schulung von Mitarbeitern

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 und Datenschutz 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 dem Auftraggeber auf Anfrage in qualifizierter Form glaubhaft gemacht oder in sonstiger Form angemessen nachgewiesen. Sollen darüber hinaus Schulungs- und Sensibilisierungsmaßnahmen beim Auftraggeber für beim Auftraggeber eingesetzte Mitarbeiter erfolgen, werden die Parteien sich über einen angemessenen Umfang und die Kostentragung einigen.

1.13 Unterstützung bei IKT-Vorfall

Der Auftragnehmer ist verpflichtet, dem Auftraggeber bei einem IKT-bezogenen Vorfall iSd Art 3 Nr. 8 DORA, der mit der bereitgestellten Leistung in Verbindung steht, Unterstützung zu leisten. Der Auftragnehmer wird für die Mitwirkung eine für die vertragliche Hauptleistung entsprechende Vergütung erhalten. Der Auftragnehmer hat jedoch den ihm entstandenen Aufwand nachzuweisen.