# Anlage zur Datenverarbeitung gemäß Art. 28 DS-GVO Vereinbarung

## Zwischen LOX24 GmbH

Seestraße 109, D-13353 Berlin, Germany, eingetragen beim Handelsregister Amtsgericht Berlin (Charlottenburg) mit der Registernummer HRB 168883 B, vertreten durch den Geschäftsführer Miguel Bastl und registriert als Telekommunikationsunternehmen im Sinne des § 2 Nr. 61 TKG.

-Auftragnehmer-

_____

_____

_____

-Auftraggeber-

über Verarbeitung personenbezogener Daten für den Auftraggeber i.S.v. Art.4 Nr.2 und Art.28 DS-GVO auf Grundlage dieses Auftrags.

### Präambel

(1) Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien gemäß Art. 28 DSGVO im Rahmen der Nutzung der Dienstleistungen von LOX24. Die Hauptleistung von LOX24 stellt eine Telekommunikationsdienstleistung im Sinne des § 2 Nr. 61 TKG dar, insbesondere die Übermittlung von Textnachrichten (z. B. SMS) über öffentliche Telekommunikationsnetze. Für diese reine Nachrichtenübermittlung gilt gemäß Art. 95 DSGVO keine Anwendung der Datenschutz-Grundverordnung, da die Verarbeitung durch das Telekommunikationsgesetz (TKG) und das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) geregelt ist. Die reine Übermittlung von Nachrichten über öffentliche Telekommunikationsnetze unterliegt nicht der DSGVO, sondern dem TKG und TDDDG. Für alle weiteren Tätigkeiten, bei denen LOX24 personenbezogene Daten speichert, verarbeitet oder analysiert (z. B. Logging, Adressbuch, Kalenderabruf, Scoring), greift die DSGVO uneingeschränkt, und LOX24 handelt in diesen Fällen als Auftragsverarbeiter gemäß Art. 28 DSGVO. Das Fernmeldegeheimnis gemäß § 3 TDDDG schützt die Vertraulichkeit der Kommunikation und steht im Vorrang vor datenschutzrechtlichen Anfragen Dritter.

(2) Diese Vereinbarung gilt jedoch für alle Nebenleistungen oder Zusatzfunktionen, bei denen LOX24 im Auftrag des Auftraggebers personenbezogene Daten verarbeitet, speichert oder analysiert, soweit diese nicht durch das TKG vollumfänglich geregelt sind. Dies betrifft insbesondere:

- die Speicherung von Nachrichten in einem Logbuch (Journal),
- die Speicherung und Verwaltung von Rufnummern und Kontaktdaten in einem Adressbuch,
- den Abruf und die Nutzung von Kalendereinträgen zur Automatisierung von Nachrichtenversand,
- die Analyse von Teilnehmerdaten zur Berechnung eines Scoring-Werts über die Anti-Betrugsschnittstelle.

Für diese Tätigkeiten ist der Auftragnehmer **Auftragsverarbeiter im Sinne von Art. 28 DSGVO**, und die vorliegende Vereinbarung regelt die diesbezüglichen Pflichten.

(3) Der Auftraggeber als Nutzer der Telekommunikationsdienstleistung wünscht Zugang zum internationalen Telekommunikationsnetz zur Übermittlung von Textnachrichten durch den Auftragnehmer an Endkunden. Die Endkunden befinden sich in einem öffentlichen Telekommunikationsnetz (Mobilfunknetz oder Festnetz) und damit in aller Regel nicht im internen Netz des Auftragnehmers.

(4) Um die jeweiligen Endkunden zu erreichen, erfolgt eine Zusammenschaltung, welche die physische und logische Verbindung öffentlicher Telekommunikationsnetze herstellt, um Nutzern eines Unternehmens die Kommunikation mit Nutzern desselben oder eines anderen Unternehmens oder die Inanspruchnahme von Diensten

eines anderen Unternehmens zu ermöglichen; Dienste können von den beteiligten Parteien erbracht werden oder von anderen Parteien, die Zugang zum Netz haben. Diese Zusammenschaltung von Telekommunikationsnetzen ist keine Beauftragung von Subunternehmen im Sinne einer Verarbeitung personenbezogener Daten, sondern ein bei Telekommunikationsdienstleistungen zwingend erforderlicher Vorgang. Der Auftraggeber hat hierbei zu beachten, dass solche Vermittlungsvorgänge auch in Drittländer erfolgen können, auch im Fall dass der Endkunde über eine europäische Rufnummer verfügt (Bsp.: Einwahl in ein Roamingnetz).

(5) Für alle Dienstleistungen welche keine Telekommunikationsleistung darstellen, gilt die nachfolgende Vereinbarung. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Hierzu zählt die Speicherung von Nachrichten, Rufnummern und Adressen in einem über das Internet abrufbaren Journal. Ebenfalls der Abruf von online Kalendereinträgen zum Zwecke der Übermittlung von Textnachrichten oder die Prüfung von personenbezogenen Daten zur Ermittlung eines Scoringwertes über die Anti-Betrugsschnittstelle.

## § 1 Gegenstand, Dauer und Spezifizierung der Verarbeitung personenbezogener Daten

(1) Der Dienstleistungsvertrag mit LOX24 beginnt durch Akzeptanz der Allgemeinen Geschäftsbedingungen bei der Anmeldung, durch Vertragsunterzeichnung oder andere schriftliche Regelung und wird, wenn nicht anders vereinbart auf unbestimmte Dauer abgeschlossen bis zu einer Kündigung des Dienstes seitens einer der Vertragspartner. Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung,
-verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

**Gegenstand**: Leistung gemäß der Servicevereinbarung als Nebenleistung zur Erbringung der Telekommunikationsdienste

**Art der Verarbeitung**: Analyse von Teilnehmerinformationen, Speicherung von Daten in Form eines Adressbuchs, Speicherung von Nachrichten in Form eines Logbuchs, Abruf und Auswertung von Google-Kalender-Einträgen, Personalisierung von SMS Texten mittels Datenbankimport.

**Kreise der betroffenen Personen**: Betroffene sind Personen, deren Daten verarbeitet werden, welche also Nachrichten erhalten oder im Adressbuch gespeichert werden und/oder Endnutzer oder Mitarbeiter und Mitglieder des Auftraggebers.

**Kategorien / Art der personenbezogenen Daten**: In Verbindung mit der erbrachten Leistung umfassen die verarbeiteten Daten Telefonnummern (Absender und Empfänger) und können je nach Fall auch Vorname, Nachname, Adresse, Standortdaten, Kontaktinformationen, und andere relevante personenbezogene Daten.

**Bearbeitungsdauer**: Begrenzt auf die Dauer der Erbringung der Services im Rahmen der Servicevereinbarung, sofern nicht zwingendes Recht oder eine Vereinbarung zwischen den Parteien vereinbart wurde.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Eine Verlagerung der Verarbeitung oder Speicherung personenbezogener Daten in ein Drittland (außerhalb der EU/EWR) bedarf der ausdrücklichen, schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Der Auftragnehmer stellt sicher, dass für jede Datenübermittlung in ein Drittland eine zulässige Rechtsgrundlage gemäß Art. 46 DSGVO vorliegt, insbesondere durch den Abschluss der von der Europäischen Kommission genehmigten Standardvertragsklauseln (SCCs) in der jeweils gültigen Fassung. Diese werden zwischen dem Auftraggeber und dem Auftragnehmer als Teil dieser Vereinbarung oder in einem gesonderten Dokument abgeschlossen und gelten als Anlage zu dieser DPA. Soweit erforderlich, ergreift der Auftragnehmer zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung, Pseudonymisierung), um das Schutzniveau der DSGVO auch bei Drittlandübermittlungen zu gewährleisten, wie vom EuGH im Urteil Schrems II (C-311/18) gefordert.Der Auftragnehmer informiert den Auftraggeber unverzüglich über relevante Änderungen in der Rechtslage oder bei Subunternehmern, die eine Neubewertung der Rechtmäßigkeit der Drittlandübermittlung erforderlich machen.

## § 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen

dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unwirksam.

## § 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung einen Verstoß gegen die Datenschutz-Grundverordnung oder sonstige datenschutzrechtliche Bestimmungen des Unionsrechts oder der Mitgliedstaaten darstellt.

(2) Bis zur Klarstellung durch den Auftraggeber darf der Auftragnehmer die beanstandete Weisung aussetzen, sofern nicht zwingende rechtliche oder technische Gründe dagegensprechen. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

(3) Der Auftragnehmer setzt technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO ein, die dem aktuellen Stand der Technik entsprechen. Der Auftraggeber bestätigt, dass er die TOMs zur Kenntnis genommen hat und im Rahmen seiner Verantwortung als Verantwortlicher prüft, ob diese für die konkrete Verarbeitungssituation ausreichen. Bei besonderen Risiken (z. B. sensible Daten, große Datenmengen) ist der Auftraggeber verpflichtet, den Auftragnehmer hierüber zu informieren, um gegebenenfalls zusätzliche Maßnahmen zu vereinbaren.

(4) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(6) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(8) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(9) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(10) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag

bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(11) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber. Die Löschung der Daten erfolgt gemäß dem Stand der Technik durch Überschreiben oder Unkenntlichmachen. Eine physische Vernichtung von Datenträgern findet nur statt, sofern dies im Hauptvertrag ausdrücklich für dedizierte Hardware vereinbart wurde.

(12) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(13) Der Auftragnehmer kann für Unterstützungsleistungen gemäß § 3, § 5 und § 6, die nicht auf einem Fehlverhalten des Auftragnehmers beruhen, eine angemessene Vergütung auf Basis des tatsächlichen Zeitaufwands verlangen.

## § 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. daten- schutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 12 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

## § 5 Anfragen Betroffener

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer ist nicht befugt, Auskunft über personenbezogene Daten zu erteilen oder Löschungen vorzunehmen, es sei denn, er erhält hierzu eine konkrete, schriftliche Weisung des Auftraggebers. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

## § 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

(4) Soweit der Auftragnehmer gemäß Art. 30 Abs. 5 DSGVO zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten verpflichtet ist, stellt er sicher, dass dieses Verzeichnis die gemäß Art. 28 Abs. 3 lit. e) DSGVO erforderlichen Informationen enthält, insbesondere:

- die Art der Verarbeitungstätigkeit,

- Kategorien betroffener Personen,
- Kategorien personenbezogener Daten,
- Empfänger oder Kategorien von Empfängern,
- geplante Speicherdauer,
- allgemeine Angaben zur internationalen Datenübermittlung,
- sowie die Kategorien von Sicherheitsmaßnahmen.

(5) Der Auftragnehmer hat das Recht, aufgrund des ihm obliegenden Fernmeldegeheimnisses nach § 3 TDDDG, die Herausgabe oder Einsicht in interne Systemdokumentationen, Netzarchitekturen, interne Sicherheitskonzepte oder sonstige betriebliche Geheimnisse abzulehnen, soweit diese nicht direkt und unmittelbar zur Erfüllung der datenschutzrechtlichen Pflichten im konkreten Auftrag erforderlich sind.

(6) Im Rahmen von Prüfungen gemäß Abs. 2 und 3 beschränkt sich die Mitwirkung des Auftragnehmers auf die Bereitstellung aggregierter, anonymisierter oder auf den konkreten Auftrag bezogener Nachweise, die keine Offenlegung von Geschäfts- oder Betriebsgeheimnissen oder sicherheitsrelevanter Infrastruktur erfordern. Insbesondere erfolgt keine Offenlegung von Systemarchitekturen, Sicherheitskonzepten Dritter oder technischen Details zu Subunternehmern, soweit diese nicht direkt Gegenstand des Auftrags sind. Der Auftragnehmer stellt auf Anfrage aggregierte, anonymisierte oder auftragsbezogene Nachweise zur Verfügung, die die Einhaltung der DSGVO belegen, ohne Betriebs- oder Sicherheitsgeheimnisse offenzulegen.

## § 7 Subunternehmer

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(4) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

a. Server-Hosting: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
b. Server-Backups: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg

(5) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.

(6) Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(7) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(8) Der Auftragnehmer behält sich vor, Subunternehmer zu wechseln, um technische, wirtschaftliche oder sicherheitstechnische Verbesserungen vorzunehmen. Der Auftraggeber wird hierüber informiert. Ein Widerspruch ist nur zulässig, wenn ein datenschutzrechtlich begründeter, konkreter Nachteil nachgewiesen wird.

## § 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Dieser Vertrag unterliegt deutschem Recht. Die Anwendung der Verordnung (EG) Nr. 593/2008 (Rome I-VO) wird vereinbart. Damit ist das gewählte Recht – soweit nicht zwingende Vorschriften eines anderen Staates (insbesondere zum Verbraucherschutz) entgegenstehen – endgültig und gegenüber Dritten durchsetzbar. Beide Parteien bestätigen, dass sie im Rahmen ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handeln und nicht als Verbraucher im Sinne der Rome I-VO gelten.

(5) Sollte eine Bestimmung dieser Vereinbarung oder eine künftige neu aufgenommene Bestimmung ganz oder teilweise unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Vertragspartner vereinbaren, die ungültige Bestimmung durch eine gültige Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Vertragspartner am besten entspricht. Das gleiche gilt im Falle einer Lücke des Vertrages.

(6) Diese Anlage ist ein Anhang zur Dienstleistungsvereinbarung. Im Falle eines Widerspruchs zwischen dieser Anlage und des Dienstleistungsvertrags gelten die Bestimmungen dieser Anlage. Alle anderen Bestimmungen und Vorschriften die nicht durch diesen Anhang geändert werden, bleiben in vollem Umfang in Kraft und wirksam mit ihren Bedingungen.

(7) Diese Anlage tritt am 23.02.2026 in Kraft. Dieser Anhang bleibt so lange in Kraft und wirksam wie der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, besitzt oder bis dieser Anhang durch einen anderen ersetzt wird.

(8) Dieser Anhang ersetzt alle vorhergehenden Auftragsdatenvereinbarungen und ersetzt damit eine Kündigung vorhergehend abgeschlossener Auftragsdatenvereinbarungen.

## §9 Haftung und Schadensersatz

(1) Die Parteien haften für Schäden aus der Verletzung datenschutzrechtlicher Pflichten nach den gesetzlichen Vorschriften, insbesondere gemäß Art. 82 DSGVO.

(2) Im Innenverhältnis zum Auftraggeber haftet der Auftragnehmer für Schäden nur dann, wenn er:

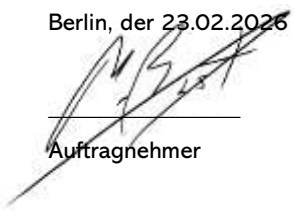
- seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder
- unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers oder gegen diese Weisungen gehandelt hat.

(3) Die Haftung des Auftragnehmers ist ausgeschlossen, sofern er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Insbesondere haftet der Auftragnehmer nicht für Schäden, die auf einer rechtswidrigen Weisung des Auftraggebers oder einer unzureichenden Mitwirkung des Auftraggebers beruhen.

(4) Soweit der Hauptvertrag Haftungsbeschränkungen enthält, finden diese auch auf die vorliegende Vereinbarung Anwendung, sofern sie mit den Anforderungen des Art. 82 DSGVO vereinbar sind. Die Haftung für Schäden, die aus der Verletzung des Lebens, des Körpers oder der Gesundheit resultieren, sowie für Schäden aus vorsätzlichen oder grob fahrlässigen Pflichtverletzungen bleibt unberührt.

(5) Der Auftraggeber stellt den Auftragnehmer von allen Ansprüchen Dritter (einschließlich Geldbußen) frei, die dadurch entstehen, dass der Auftraggeber seine Pflichten als Verantwortlicher verletzt hat, insbesondere bei fehlender Rechtsgrundlage für die Datenübermittlung oder bei rechtswidrigen Weisungen.

Berlin, der 23.02.2026 _____der _____



_____ _____

Auftragnehmer Auftraggeber

Anlage: Technische und organisatorische Maßnahmen

## Anlage zum Auftrag gemäß Art. 28 DS-GVO Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

(1) Innerhalb seines Verantwortungsbereiches ergreift der Auftragnehmer die folgenden Einzelmaßnahmen zur Erreichung der Ziele dieser Vereinbarung und der rechtlichen Anforderungen:

### I. Vertraulichkeit

- Zutrittskontrolle der Datacenterparks in Nürnberg und Falkenstein
    - Elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenterpark
    - Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Mitarbeiters unseres Dienstleisters
- Zutrittskontrolle der Verwaltung
    - Zutrittskontrollsystem mit Protokollierung
    - Mechanische Zugangskontrolle
    - Zugang für Gäste nur in Anwesenheit eines LOX24 Mitarbeiters
- Server Zugang
    - Server-Passwörter, welche nur einen kleinen Kreis von geschulten Mitarbeitern zugänglich sind
    - Zugangsprotokollierung auf dem Sever (Zugriffskontrolle)
    - Richtlinien zur Vergabe von sicheren Passwörtern. Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- Datenträgerkontrolle
- Trennungskontrolle
- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Pseudonymisierung
- Web-Account/Journal
    - passwortgeschützten Web-Account
    - Zweifaktorauthentifizierung per Mail oder Telefonanruf
    - TLS 1.2 oder höher verschlüsselte Übertragung vom LOX24-Server
    - Verschlüsselung der Daten in einer gesicherten Datenbank nach „Stand der Technik“

### II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- Eingabekontrolle
- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.

- Änderungen der Daten werden protokolliert.
- Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

### III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) • Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Monitoring aller relevanten Server.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.
- Backup- und Recovery-Konzept mit täglicher Sicherung der Daten
- Einsatz von Festplattenspiegelung.
- Einsatz von Softwarefirewall und Portreglementierungen.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

### IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das
- Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Auftragskontrolle
- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.

(2) Die Einzelmaßnahmen werden der IT-technischen Entwicklung sowie der sich daraus ergebenden Veränderung der IT-Landschaft des Auftragnehmers laufend angepasst.