Datenverarbeitungsvereinbarung

DIESE DATENVERARBEITUNGSVEREINBARUNG („DVV“) WIRD ZWISCHEN DER ANYBILL GMBH, TÜRKENSTRASSE 95, 80799 MÜNCHEN, DEUTSCHLAND („ANYBILL“; IM FOLGENDEN AUCH: AUFTRAGSVERARBEITER) UND DEM IM PARTNER BEITRITTS-FORMULAR („PARTNER“; IM FOLGENDEN AUCH: VERANTWORTLICHER) GESCHLOSSEN. DIESE DVV WURDE DURCH VERWEIS IN DIE ANYBILL-PARTNERVEREINBARUNG („VEREINBARUNG“) AUFGENOMMEN UND BILDET EINEN INTEGRALEN BESTANDTEIL DERSELBEN. ALLE HIERIN VERWENDETEN BEGRIFFE HABEN DIE IHNEN IM GLOSSAR ZUGEWIESENE BEDEUTUNG. DIE BEDINGUNGEN DIESER DVV SIND MIT DEM DATUM DES INKRAFTTRETENS FÜR DIE PARTEIEN RECHTSVERBINDLICH.

Präambel

Die Parteien schließen diesen AVV im Zusammenhang mit der in der Leistungsbeschreibung geregelten Zusammenarbeit und zur Erfüllung der Vorgaben gemäß Art. 28 DS-GVO.

I. Allgemeine Verantwortlichkeiten der Parteien

(1) **Auftragsverarbeitungs-Verhältnis.** Die Bereitstellung der Services für den Verantwortlichen kann (a) die Verarbeitung bestimmter Daten erfordern, die zu Zwecken und mit Mitteln erhoben und verarbeitet werden, die allein von dem Verantwortlichen bestimmt werden („Daten des Verantwortlichen“) und/oder (b) erfordern, dass Daten des Verantwortlichen dem Auftragsverarbeiter zur Verfügung gestellt oder zugänglich gemacht werden. Wenn und soweit diese Daten des Verantwortlichen aus personenbezogenen Daten im Sinne der Datenschutzgesetze bestehen oder solche enthalten („personenbezogene Daten des Verantwortlichen“), wird der Auftragsverarbeiter in Bezug auf diese Daten als Auftragsverarbeiter handeln, während der Verantwortliche für diese Daten der Verantwortliche bleibt.

(2) **Pflichten des für die Verarbeitung Verantwortlichen.** Im Rahmen der Zusammenarbeit übermittelt der Verantwortliche dem Auftragsverarbeiter die personenbezogenen Daten des Verantwortlichen, stellt diese zur Verfügung oder macht sie ihm zugänglich. Der Verantwortliche ist allein für die Rechtmäßigkeit der Übermittlung (insbesondere für Rechtsgrundlage, Information der Betroffenen und Datenminimierung) und der Zwecke der Verarbeitung verantwortlich.

(3) **Verantwortlichkeiten von anybill als Auftragsverarbeiter.** In der Funktion als Auftragsverarbeiter verarbeitet Anybill personenbezogene Daten des Verantwortlichen im Auftrag des Verantwortlichen nur gemäß den Bestimmungen dieses AVV und den dokumentierten Weisungen des Verantwortlichen. Ist Anybill verpflichtet, personenbezogene Daten des Verantwortlichen nach dem für ihn geltenden Recht der EU oder der EU-Mitgliedstaaten auf andere Weise zu verarbeiten, als er vom Verantwortlichen angewiesen wurde, so hat er den Verantwortlichen zu unterrichten, bevor diese Verarbeitung erfolgt, es sei denn, das für die Verarbeitung geltende Recht verbietet Anybill die Unterrichtung des Verantwortlichen aus einem wichtigen Grund des öffentlichen Interesses. Anybill stellt sicher und überprüft regelmäßig, dass die Verarbeitung personenbezogener Daten des Verantwortlichen in seinem Verantwortungsbereich, einschließlich der gemäß dieses AVV Annex 3 eingesetzten Unterauftragsverarbeiter, im Einklang mit den Bestimmungen dieses AVV, mit den geltenden Datenschutzgesetzen und insbesondere mit der DS-GVO durchgeführt wird.

II. Einzelheiten der Verarbeitung

(1) **Festlegung der Einzelheiten.** Die Einzelheiten der Verarbeitung und Verantwortlichkeiten werden für die Bereitstellung der Belege sowie weitere Leistungen für den Händlerpartner gemäß der Leistungsbeschreibung in Annex 2 festgelegt; die Einzelheiten der Verarbeitung und Verantwortlichkeiten werden für die digitale Belegausgabe über ein Zahlungsmittel eines Partners in Annex 3 festgelegt; die Annex enthalten Bestimmungen über die an der Verarbeitung beteiligten Parteien, die Art, den Zweck und den Gegenstand der Verarbeitung, die Dauer der Verarbeitung, die Kategorien der betroffenen Personen und die Arten der betroffenen personenbezogenen Daten des Verantwortlichen.

(2) **Laufzeit.** Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

III. Ort der Verarbeitung; Übermittlung in Drittländer

(1) **Ort der Verarbeitung.** Die personenbezogenen Daten des Verantwortlichen werden vom Auftragsverarbeiter in seinen eigenen Räumlichkeiten oder in den Räumlichkeiten seines beauftragten Unterauftragnehmers verarbeitet. Personenbezogene Daten werden ausschließlich in der EU oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeitet.

(2) **Übermittlung in Drittländer.** Eine Verarbeitung personenbezogener Daten des Verantwortlichen außerhalb der EU/des EWR ist nur auf entsprechende Weisung des Verantwortlichen und nur dann zulässig, wenn die Voraussetzungen gemäß Ziffer VIII Satz 1 dieser DVV erfüllt sind.

IV. Weisungen des Verantwortlichen

(1) **Allgemeine Weisungen.** Die Parteien sind sich darüber einig und der Verantwortliche nimmt zur Kenntnis, dass die Bestimmungen dieser DVV die allgemeinen Weisungen des Verantwortlichen bezüglich der Verarbeitung personenbezogener Daten des Verantwortlichen enthalten. Der Verantwortliche kann dem Auftragsverarbeiter jederzeit spezifische Weisungen erteilen, die zur Einhaltung der Datenschutzgesetze erforderlich sind.

(2) **Abweichende Weisungen.** Einzelne Weisungen, die von den Bestimmungen dieser DVV abweichen oder die dem Auftragsverarbeiter zusätzliche Anforderungen auferlegen, bedürfen der vorherigen Zustimmung des Auftragsverarbeiters.

(3) **Einhaltung der Datenschutzgesetze.** Der Verantwortliche stellt sicher, dass ihre spezifischen Weisungen in Bezug auf die personenbezogenen Daten des Verantwortlichen mit den Datenschutzgesetzen übereinstimmen und dass die Verarbeitung der personenbezogenen Daten des Verantwortlichen gemäß den Weisungen des Verantwortlichen nicht dazu führt, dass der Auftragsverarbeiter gegen die Datenschutzgesetze und insbesondere gegen die DS-GVO verstößt. Ist der Auftragsverarbeiter der Ansicht, dass eine zulässige spezifische Weisung gegen geltende Datenschutzgesetze verstößt, so teilt er dies dem Verantwortlichen so schnell wie möglich mit. Darüber hinaus ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung auszusetzen, bis der Verantwortliche die Weisung bestätigt.

(4) **Textform.** Besondere Weisungen des Verantwortlichen erfolgen grundsätzlich in Textform durch die nach der Leistungsbeschreibung hierzu befugten Personen des Verantwortlichen. Mündliche Weisungen bedürfen zu ihrer Wirksamkeit der unverzüglichen schriftlichen oder in Textform erfolgenden Bestätigung durch den Verantwortlichen.

V. Unter-Auftragsverarbeiter

(1) **Vorab genehmigte Unter-Auftragsverarbeiter.** Der Auftragsverarbeiter darf ohne vorherige schriftliche Zustimmung des Verantwortlichen keine Aufträge zur Unter-Auftragsverarbeitung erteilen. Der Verantwortliche erteilt dem Auftragsverarbeiter die Erlaubnis, Verarbeitungsvorgänge an die in der Leistungsbeschreibung aufgeführten Unter-Auftragsverarbeiter zu vergeben. ANYBILL verwendet derzeit die in Annex 3 aufgeführten Unter-Auftragsverarbeiter. Der Partner stimmt dem Einsatz dieser Unter-Auftragsverarbeiter zu.

(2) **Haftung des Auftragsverarbeiters.** Der Auftragsverarbeiter muss allen Unter-Auftragsverarbeitern Datenschutz-, Vertraulichkeits- und Datensicherheitsverpflichtungen auferlegen, die (a) den Anforderungen der Art. 28 und 29 DS-GVO entsprechen und (b) mindestens so streng sind wie die in dieser DVV festgelegten Verpflichtungen. Kommt ein Unter-Auftragsverarbeiter seinen Datenschutzverpflichtungen in Bezug auf die Verarbeitung personenbezogener Daten nicht nach, bleibt der Auftragsverarbeiter gegenüber dem Verantwortlichen in vollem Umfang für die Erfüllung der Verpflichtungen dieses Unter-Auftragsverarbeiters haftbar.

(3) **Einsatz von Unter-Auftragsverarbeitern.** Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens dreißig (30) Kalendertage vor dem geplanten Einsatz eines neuen Unter-Auftragsverarbeiters in Textform über die beabsichtigte Ernennung. Teilt der Verantwortliche dem Auftragsverarbeiter innerhalb von dreißig (30) Kalendertagen nach Erhalt dieser Mitteilung aus sachlich gerechtfertigten Gründen, insbesondere aufgrund datenschutzrechtlicher Bedenken, schriftlich seine Einwände gegen die vorgeschlagene Ernennung mit, handeln die Parteien nach Treu und Glauben eine für beide Seiten akzeptable und datenschutzkonforme Alternative aus. Wird eine solche Alternative nicht innerhalb von zwei (2) Monaten nach dem Einspruch vereinbart, hat der Verantwortliche das Recht, die Services in dem Umfang zu beenden, in dem sie den Einsatz des vorgeschlagenen Unter-Auftragsverarbeiters erfordern.

(4) **Unter-Auftragsverarbeiter in Drittländern.** Ungeachtet der Regelungen in Ziffer VIII Satz 1 dieser DVV setzt die Beauftragung eines Unter-Auftragsverarbeiters in einem Drittland die ausdrückliche Zustimmung des Verantwortlichen zur Beauftragung dieses Unter-Auftragsverarbeiters voraus.

VI. Anfragen betroffener Personen

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Beschwerde, Mitteilung oder Anfrage, die er direkt von einer betroffenen Person erhalten hat und die deren personenbezogene Daten betrifft, ohne auf diese Anfrage zu reagieren, es sei denn, der Auftragsverarbeiter wurde vom Verantwortlichen anderweitig dazu ermächtigt. Der Auftragsverarbeiter unterstützt den Verantwortlichen in angemessener Weise bei allen Beschwerden, Mitteilungen oder Anträgen, die er von einer betroffenen Person erhält, gegen eine Vergütung, die gemäß dem Auftrag zu berechnen ist, sofern und soweit die Unterstützung nicht aufgrund eines vom Auftragsverarbeiter zu vertretenden Verstoßes gegen gesetzliche oder vertragliche Pflichten erforderlich wird.

VII. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter setzt während der Laufzeit dieses AVV angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO um und hält diese aufrecht. Die jeweils geltenden Maßnahmen sind in Annex 4 beschrieben und Bestandteil dieses AVV.

(2) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen in den Betriebsräumen des Auftragnehmers durchzuführen oder von im Einzelfall zu benennenden Prüfern durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mindestens vier Wochen zuvor anzumelden sind, von der Einhaltung dieses Vertrags durch den Auftragnehmer in dessen Geschäftsbetrieb während der Geschäftszeiten zu überzeugen. Solche Überprüfungen finden maximal einmal im Jahr statt.

(3) 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 vertraglich vereinbarten technischen und organisatorischen Maßnahmen nachzuweisen.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(5) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine angemessene Vergütung geltend machen.

VIII. Übermittlung in Drittländer

(1) **Voraussetzungen.** Der Auftragsverarbeiter darf personenbezogene Daten nur dann in ein Drittland übermitteln, wenn die Voraussetzungen der Art. 44 ff. DS-GVO oder vergleichbare Bestimmungen der geltenden Datenschutzgesetze erfüllt sind.

(2) **(Unter-)Verarbeiter in Drittländern.** Die Bestimmungen dieses Ziffer VIII Satz 1 gelten auch, wenn der Auftragsverarbeitereinen (Unter-)Verarbeiter in einem Drittland beauftragt.

IX. Unterstützung

(1) **Ermittlungen einer Aufsichtsbehörde.** Die Parteien leisten einander Beistand im Falle einer Untersuchung oder eines Ersuchens einer Regulierungsbehörde, einschließlich einer Aufsichtsbehörde, oder einer ähnlichen Behörde. Ist eine Partei von einer Untersuchung oder einem Ersuchen einer Regulierungsbehörde, einschließlich einer Aufsichtsbehörde oder einer ähnlichen Behörde, betroffen, so unterrichtet sie die anderen Parteien unverzüglich davon, sofern dies zulässig ist, und arbeitet im Rahmen einer solchen Untersuchung oder eines solchen Ersuchens mit ihnen zusammen.

(2) **Datenschutzvorfälle.** Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von vierundzwanzig (24) Stunden nach der Entdeckung, wenn eine Sicherheitsverletzung (**„Sicherheitsvorfall“**) festgestellt wird, insbesondere wenn ein solcher Sicherheitsvorfall zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Weitergabe oder zum unbefugten Zugriff auf personenbezogene Daten, die die Parteien im Rahmen dieser DVV verarbeiten, geführt hat oder führen könnte. Diese Meldung kann zunächst in zusammengefasster Form erfolgen und muss zumindest die dem Auftragsdatenverarbeiter zu diesem Zeitpunkt bekannten Informationen enthalten. Die Meldung soll die in Art. 33 Abs. 3 DS-GVO genannten Angaben umfassen oder - falls der Auftragsverarbeiter nicht in der Lage ist, diese Informationen vollständig bereitzustellen, eine Erläuterung enthalten
(a) der Gründe für diese Unfähigkeit,

(b) der voraussichtlichen zusätzlichen Zeit, die für die Vervollständigung der Informationen benötigen wird, und
(c) der Auswirkungen dieser Unfähigkeit auf die Maßnahmen zur Abmilderung der nachteiligen Auswirkungen des Sicherheitsvorfalls, soweit vorhanden.
Ist der Verantwortliche infolge eines Sicherheitsvorfalls aufgrund eines Risikos für die Rechte und Freiheiten natürlicher Personen gesetzlich verpflichtet, Informationen bereitzustellen (insbesondere, aber nicht ausschließlich, aufgrund der Informationspflichten gemäß Art. 33, 34 DS-GVO), so unterstützt der Auftragsverarbeiter den Verantwortlichen auf dessen Ersuchen hin bei der Erfüllung seiner Informationspflichten, soweit dies angemessen und erforderlich ist.

(3) **Datenschutz-Folgenabschätzung.** Die Parteien arbeiten zusammen und unterstützen sich gegenseitig unter Berücksichtigung der Art der Verarbeitung und der jeweiligen Partei zur Verfügung gestellten Informationen bei den in Art. 35 DS-GVO genannten Datenschutz-Folgenabschätzungen oder bei allen regulatorischen Konsultationen, zu denen eine Partei im Hinblick auf eine solche Datenschutz-Folgenabschätzung gemäß Art. 36 DS-GVO gesetzlich verpflichtet ist.

(4) **Abweichende rechtliche Vorgaben.** Unbeschadet jeglicher Haftungsverpflichtung von ANYBILL wird der PARTNER, um die nachteiligen Auswirkungen einer solchen Entdeckung bestmöglich abzumildern, ANYBILL unverzüglich informieren, wenn Nutzungsdaten oder aggregierte Daten nach den Datenschutzgesetzen eine Datenkategorie darstellen, aus ihr bestehen oder sie enthalten würden, deren Verarbeitung durch ANYBILL in Übereinstimmung mit diesen Datenschutzgesetzen dem PARTNER, ANYBILL oder beiden Parteien weitere Verpflichtungen auferlegen würde.

X. Auditrechte

(1) **Vor-Ort-Audits.** Der Verantwortliche ist berechtigt, während der üblichen Geschäftszeiten (Montag bis Freitag von 9.00 bis 18.00 Uhr) auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Wahrung von Geschäftsgeheimnissen die Geschäftsräume des Auftragsverarbeiters, in denen personenbezogene Daten verarbeitet werden, zu betreten, um die Einhaltung der vorliegenden DVV zu überprüfen. Der Verantwortliche informiert den Auftragsverarbeiter rechtzeitig (in der Regel mindestens zwei Wochen im Voraus) über alle Umstände, die mit der Durchführung eines Audits zusammenhängen.

(2) **Auditberichte.** Zusätzlich zu den dem Verantwortlichen zustehenden Kontroll- und Auditrechten gemäß Art. 28 Abs. 3 lit. h DS-GVO kann der Nachweis der Einhaltung dieser DVV auch durch die Einhaltung eines genehmigten Verhaltenskodex gemäß Art. 40 DS-GVO, eine Zertifizierung nach einem anerkannten Zertifizierungsverfahren gemäß Art. 42 DS-GVO und die Vorlage geeigneter, aktueller Zertifikate, Berichte oder Berichtsauszüge unabhängiger Stellen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder durch eine geeignete Bescheinigung nach einem IT-Sicherheits- oder Datenschutzaudit („Auditbericht“) nachgewiesen werden, soweit und sofern sich der Verantwortliche anhand dieser Nachweise in geeigneter Weise von der Einhaltung der vorliegenden DVV durch den Auftragsverarbeiter überzeugen kann.
Die Parteien vereinbaren, dass der Auftragsverarbeiter dem Verantwortlichen auf Anfrage geeignete und aktuelle Nachweise zur Verfügung stellt, die die Einhaltung der datenschutzrechtlichen Anforderungen und der DVV belegen. Die Vorlage solcher Nachweise berührt das Kontroll- und Auditrecht des Verantwortlichen nicht, kann jedoch bei der Festlegung von Art, Umfang, Häufigkeit und Durchführung von Audits angemessen berücksichtigt werden.

XI. Rückgabe oder Löschung personenbezogener Daten des Verantwortlichen

Auf schriftliches Verlangen des Verantwortlichen während der Laufzeit der jeweiligen Leistungsbeschreibung oder bei Beendigung oder Ablauf einer solchen Leistungsbeschreibung und wenn der Auftragsverarbeiter nicht mehr verpflichtet ist, die personenbezogenen Daten des Verantwortlichen ganz oder teilweise aufzubewahren, um die Services zu erbringen (z.B. um die Integrität der Daten des Verantwortlichen zu wahren), hat der Auftragsverarbeiter auf entsprechende Weisung des Verantwortlichen die personenbezogenen Daten des Verantwortlichen zurückzugeben oder zu vernichten. Wenn Datenschutzgesetze, denen der Auftragsverarbeiter unterliegt, den Auftragsverarbeiter daran hindern, die personenbezogenen Daten des Verantwortlichen ganz oder teilweise zurückzugeben oder zu vernichten, muss der Auftragsverarbeiter gewährleisten, dass (a) die Vertraulichkeit dieser

personenbezogenen Daten des Verantwortlichen gewahrt bleibt, (b) er diese personenbezogenen Daten des Verantwortlichen nicht mehr aktiv verarbeitet und (c) er diese personenbezogenen Daten des Verantwortlichen zurückgibt oder vernichtet, sobald die gesetzliche Verpflichtung, personenbezogenen Daten des Verantwortlichen nicht zurückzugeben bzw. zu vernichten, nicht mehr besteht.

XII. Sonstiges

(1) **Keine (Unter-)Auftragsverarbeitung.** Dienstleister, die keinen Zugriff auf personenbezogene Daten nehmen oder rein technische Hilfstätigkeiten ausüben, gelten nicht als Auftragsverarbeiter nach diesem AVV.

(2) **Anwendbares Recht.** Diese DVV unterliegt deutschem Recht, ohne Berücksichtigung der Rechtswahl- oder Kollisionsnormen jeglicher Rechtsordnung. Verweise auf die Geltung gesetzlicher Vorschriften haben nur klarstellende Bedeutung. Auch ohne eine derartige Klarstellung gelten die gesetzlichen Vorschriften, soweit sie in dieser DVV nicht abgeändert oder ausdrücklich ausgeschlossen werden.

(3) **Eskalationsverfahren.** Abschnitt 15 der Vereinbarung gilt entsprechend für alle Streitigkeiten oder Ansprüche, die sich aus dieser DVV ergeben oder mit ihr in Zusammenhang stehen.

(4) **Gerichtsstand.** Alle Streitigkeiten, Klagen, Ansprüche oder Klagegründe, die sich aus oder in Verbindung mit dieser DVV ergeben, unterliegen der ausschließlichen Zuständigkeit der Gerichte in München, Deutschland (Landgericht München I).

(5) **Erfordernis der Schriftform.** Änderungen oder Ergänzungen dieser DVV bedürfen zu ihrer Wirksamkeit der Schriftform und der Unterzeichnung durch die Parteien. Wird in dieser DVV die „Schriftform“ verlangt oder ist in dieser DVV bestimmt, dass Erklärungen der Parteien „schriftlich“ abzugeben sind, so ist die Schriftform im Sinne des § 126 BGB gemeint. Die Übermittlung per Telefax wahrt die vereinbarte Form, ebenso die Übermittlung elektronischer, gegen Bearbeitung geschützter Dokumente (z.B. PDF-Dateien) oder elektronischer Nachrichten, die über die ANYBILL Solution versandt werden, auch wenn sie nicht handschriftlich unterschrieben oder mit einem Unterschriftsstempel oder einer sonstigen gedruckten oder eingescannten Unterschrift versehen sind. Der Versand einer einfachen E-Mail oder einer anderen elektronischen Nachricht, die nicht über die ANYBILL Solution versandt wird, entspricht jedoch nicht der vereinbarten Form.

(6) **Salvatorische Klausel.** Sollte eine Bestimmung dieser DVV von einem zuständigen Gericht für ungültig oder nicht durchsetzbar befunden werden, bleiben alle anderen Bestimmungen in vollem Umfang in Kraft und wirksam.

ANNEX 1 – Gegenstand des Auftrags Basis-Beleg

Gegenstand und Zweck der Verarbeitung

Anybill verarbeitet für den Partner („Händlerpartner") Daten zum Zweck der Erstellung und Bereitstellung von digitalen Kassenbelegen und unterstützt den Partner somit bei der Umsetzung seiner Verpflichtung nach § 146a Abs. 2 S. 1 AO. Soweit im Hauptvertrag vereinbart, verarbeitet Anybill für den Partner darüber hinaus Daten zum Zweck der Erstellung und Bereitstellung eines Archivs der Zahlungsbelegen nach der Leistungsbeschreibung des Produktes "Händlerzahlungsbelegarchivs". Soweit im Hauptvertrag vereinbart, verarbeitet Anybill für den Partner darüber hinaus Daten zum Zweck des Speicherns und Versendens von E-Mail-Adressen sowie weiterer Teile der Leistungsbeschreibung "Marketingoptionen".

Art(en) der personenbezogenen Daten

Folgende Datenarten sind Gegenstand dieses Auftrags:

- Belegdaten (z.B. Angaben nach § 6 KassenSicherungsVO)
- Eindeutige Kennnummern des Auftraggebers (z.B. Kundenkarten-ID)
- Eindeutige Kennnummern von anybill (z.B. anybill User-ID)
- E-Mail-Adresse (Wenn durch Funktionsbereitstellung vereinbart)
- IT-Nutzungsdaten

Besondere Kategorien personenbezogener Daten (bspw. Gesundheitsdaten, Daten über die rassische / ethnische Herkunft) werden im Rahmen des Auftragsverarbeitungsverhältnisses nicht verarbeitet.

Kategorien betroffener Person

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

- Mitarbeiter des Auftraggebers/des Verantwortlichen
- Kunden des Auftraggebers/des Verantwortlichen

ANNEX 2 – Gegenstand des Auftrags Card-Linked (Issuer)

Gegenstand und Zweck der Verarbeitung

Anybill verarbeitet für den Partner, der das Zahlungsmittel zur Verfügung stellt, Daten zum Zwecke der Bereitstellung und Übermittlung von digitalen Kassenbelegen sowie Verknüpfung mit einem bereits bestehenden Bankkonto.

Art(en) der personenbezogenen Daten

Folgende Datenarten sind Gegenstand dieses Auftrags:

- Belegdaten (z.B. Angaben nach § 6 KassenSicherungsVO)
- Eindeutige Kennnummern des Auftraggebers
- Eindeutige Kennnummern von anybill (z.B. anybill User-ID)
- IT-Nutzungsdaten
- Personen und Kontaktdaten (z.B. Name und Adresse des Kunden)

Besondere Kategorien personenbezogener Daten (bspw. Gesundheitsdaten, Daten über die rassische / ethnische Herkunft) werden im Rahmen des Auftragsverarbeitungsverhältnisses nicht verarbeitet.

Kategorien betroffener Person

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

- Kunden des Auftraggebers/des Verantwortlichen

ANNEX 3 – Unter-Auftragsverarbeiter

ANYBILL setzt zurzeit die folgenden Unter-Auftragsverarbeiter ein:

Unter-Auftragsverarbeiter	**Zweck der Verarbeitung**	**Drittlandsübermittlung**
Allgemein		
Microsoft Azure Microsoft Ireland Operations Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland Der Unterauftragsverarbeiter Microsoft Ireland Operations Limited erbringt die Leistungen im Rahmen von Microsoft Azure; die Verarbeitung der personenbezogenen Daten erfolgt dabei in einem in Deutschland betriebenen Tenant (Microsoft Germany).	Speicherung digitaler Kassenbelege	Daten werden in die USA übermittelt. Wir haben Standardvertragsklauseln mit Microsoft vereinbart (standard data protection clauses). Außerdem hat Microsoft zusätzliche Sicherheitsmaßnahmen implementiert (additional safeguards). Für die USA liegt ein Angemessenheitsbeschluss vor. Die Microsoft Corporation ist unter dem EU-U.S. Data Privacy Framework zertifiziert und die verwendete Datenkategorie ist von der Zertifizierung umfasst.
Mailjet Mailgun Technologies Inc., 112 E Pecan St #1135, San Antonio, TX 78205, USA	Versand von digitalen Kassenbelegen	Daten werden in die USA übermittelt. Wir haben Standardvertragsklauseln mit Mailjet vereinbart (standard data protection clauses).
Datadog Datadog Inc., 620 8th Ave, 45th Fl, New York, NY 10018 USA	Verarbeitung technischer Logs	Daten werden in die USA übermittelt. Datadog ist mit dem EU-U.S. Data Privacy Framework (EU-U.S. DPF) vereinbar und entspricht der GDPR: https://www.datadoghq.com/legal/privacy/#supplemental-notice-for-the-eea-uk-and-switzerland
Freshworks, Inc., 2950 S. Delaware Street, Suite 201, San Mateo, California 94403, USA	E-Mail-Ticketingsystem	Daten werden in die USA übermittelt. Verarbeitung der Daten nach EU US Data Privacy Framework: https://www.freshworks.com/privacy/

ANNEX 4 – Technische und Organisatorische Maßnahmen

ANYBILL hat die folgenden technischen und organisatorischen Maßnahmen im Einklang mit Art. 32 Abs. 1 lit. b DS-GVO getroffen.

	Ist ein Sicherheitskonzept nach Art. 32 DS-GVO vorhanden?	Ja. anybill verfügt über ein Informationssicherheitskonzept gemäß Art. 32 DS-GVO, das im Rahmen eines Information Security Management Systems (ISMS) umgesetzt ist. Das ISMS orientiert sich an den Anforderungen der ISO/IEC 27001 und stellt sicher, dass Risiken systematisch bewertet, geeignete Schutzmaßnahmen implementiert und Prozesse zur Informationssicherheit kontinuierlich verbessert werden. Kunden profitieren von einem hohen Maß an Datensicherheit, Transparenz und Compliance auch im Hinblick auf regulatorische Vorgaben.
	Wurden Maßnahmen zur physischen Zutrittskontrolle ergriffen, die verhindern, dass Unbefugte physisch auf Systeme, Datenverarbeitungsanlagen oder -vorgänge zugreifen können?	Ja. Maßnahmen Büroräume: - Zutrittskontrollsysteme, Leser (Chipkarte/NFC-Token) - Schlüsselverwaltung/Dokumentation der Schlüsselausgabe - Sicherung von Türen (elektrische Türöffnung, Zahlenschlösser, etc.) - Videoüberwachung im Eingangsbereich - Büro für interne Sicherheit, Pförtner - Alarmsystem bzw. Einbruchmeldeanlage Maßnahmen Serverräume: - Die physische Zutrittskontrolle wird vollständig durch Microsoft im Rahmen der Azure-Cloud-Infrastruktur gewährleistet. Die Rechenzentren von Microsoft unterliegen strengen physischen Sicherheitsmaßnahmen (u. a. mehrstufige Zugangskontrollen, Videoüberwachung, Sicherheitspersonal und Zutrittsprotokollierung) und sind nach internationalen Standards wie ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 zertifiziert. Ein physischer Zugriff durch anybill-Mitarbeitende oder sonstige Unbefugte auf Systeme oder Datenverarbeitungsanlagen ist ausgeschlossen.
	Sind Maßnahmen der logischen Zugriffskontrolle implementiert, die den Zugriff Unbefugter auf Datenverarbeitungs-systeme verhindern?	Ja. - Persönliches und individuelles Login für die Nutzung von Systemen oder Firmennetzwerken und ggf. weitere Zugangskennungen - Passwortvergabe (Definition von Passwortanforderungen hinsichtlich Komplexität und Aktualisierungsintervallen) Single Sign-on - Separate Systemanmeldung für bestimmte Anwendungen - Automatisches Schließen von Programmen nach einer bestimmten Zeit ohne Benutzeraktivität (ebenso passwortgeschützter Bildschirmschoner oder automatische Einrichtung von Arbeitspausen) - Elektronische Dokumentation aller Passwörter und Verschlüsselung dieser Dokumentation zum Schutz vor unberechtigtem Zugriff - Personalisierte Chipkarten/NFC-Token etc.

		- Sicherheitsschulungen und Gewährleistung der Aufmerksamkeit der Mitarbeiter (einschließlich Schulungen zu Phishing und Social Engineering) - Der Zugang zu Systemen und Daten erfolgt ausschließlich über personalisierte, rollenbasierte Benutzerkonten mit Fokus auf Multi-Faktor-Authentifizierung (MFA). - Passwort- und Zugriffsvorgaben richten sich nach den Microsoft Entra ID-(Azure AD)-Richtlinien und anybills interner Security Policy. - Administrative Zugriffe werden protokolliert, regelmäßig überprüft und nach dem Least-Privilege-Prinzip vergeben.
	Wurden Maßnahmen zur Kontrolle des Datenzugriffs ergriffen, die sicherstellen, dass nur berechtigte Personen Zugang zu den Daten haben, die in ihren Zugriffsrechten enthalten sind, und dass diese Personen nur begrenzten Zugang zu den Daten haben?	Ja. Maßnahmen: - Zugriffsrechte auf Datenbestände werden strikt nach Rollen- und Berechtigungskonzept vergeben und regelmäßig überprüft. - Mitarbeitende dürfen personenbezogene Daten ausschließlich im Rahmen ihrer Aufgaben und nach entsprechender Vertraulichkeitsverpflichtung verarbeiten.
	Wurden Maßnahmen zur Kontrolle von Datenübermittlungen ergriffen, die die Vertraulichkeit und Integrität personenbezogener Daten bei der Übermittlung sowie die Übermittlung von Datenträgern sicherstellen?	Ja. anybill stellt sicher, dass alle Datenübermittlungen ausschließlich über verschlüsselte Kommunikationskanäle erfolgen (z. B. TLS 1.2+, HTTPS, SFTP, VPN). - Zur Wahrung der Vertraulichkeit und Integrität personenbezogener Daten werden zusätzlich starke Passwortrichtlinien und verschlüsselte Dateiformate verwendet, sofern ein elektronischer Datenaustausch außerhalb der automatisierten Systemkommunikation erfolgt (z. B. bei einmaligem Datenaustausch mit Partnern). - Alle Passwörter werden getrennt vom jeweiligen Datenträger oder Kommunikationskanal übermittelt. - Ein physischer Versand von Datenträgern findet grundsätzlich nicht mehr statt; sollte dies ausnahmsweise erforderlich sein, erfolgt die Übermittlung ausschließlich verschlüsselt, passwortgeschützt und nachvollziehbar protokolliert.
	Wurden Maßnahmen implementiert, die verhindern, dass unbefugte Personen auf gespeicherte personenbezogene Daten zugreifen, diese kopieren, verändern oder löschen können – unabhängig vom verwendeten physischen oder virtuellen Speicherort?	Ja. - Daten werden ausschließlich in der Microsoft Azure-Cloud verarbeitet und sind sowohl bei Speicherung (at rest) als auch bei Übertragung (in transit) verschlüsselt (AES-256 / TLS 1.2+). - Der Zugriff auf Daten erfolgt nur über authentifizierte, rollenbasierte Benutzerkonten mit Multi-Faktor-Authentifizierung. - Physische Datenträger werden von anybill nicht mehr genutzt; der Schutz der Azure-Infrastruktur und Datenträger erfolgt gemäß den ISO/IEC 27001, 27017 und 27018-Zertifizierungen von Microsoft.
	Wurden Maßnahmen zur Verhinderung der unbefugten Eingabe von Daten sowie des unbefugten Zugriffs, der unbefugten Änderung und der	Ja. - Der Zugriff auf Systeme und Daten erfolgt ausschließlich über personalisierte, rollenbasierte Benutzerkonten, - Multi-Faktor-Authentifizierung (MFA) mittels Microsoft Entra ID (Azure AD)

	unbefugten Löschung von gespeicherten personenbezogenen Daten ergriffen?	- Eingaben und Änderungen in produktiven Systemen sind nur für autorisierte Benutzer über freigegebene Anwendungen und gesicherte Schnittstellen (API, Web-UI) möglich.
	Wurden Maßnahmen zur Kontrolle der Dateneingabe ergriffen, die es ermöglichen festzustellen, wer auf personenbezogene Daten zugegriffen, sie verändert, gelöscht oder übertragen hat und auf welche Weise?	Ja. - Zugriffe, Änderungen und Übertragungen werden protokolliert (Logging) innerhalb der Microsoft-Azure-Infrastruktur. - Die Logs enthalten u. a. Benutzerkennung, Zeitpunkt, Art des Zugriffs und betroffene Datenobjekte. - Der Zugriff auf Protokolldaten ist rollenbasiert beschränkt und erfolgt nur durch autorisierte Personen (z. B. Security- oder Compliance-Beauftragte). - Änderungen an Daten in Produktivsystemen erfolgen ausschließlich über authentifizierte Benutzerkonten mit Multi-Faktor-Authentifizierung (MFA) über Microsoft Entra ID (Azure AD). - Datenänderungen und Systemänderungen werden zusätzlich über kontrollierte CI/CD-Prozesse mit Freigabe- und Review-Schritten nachvollziehbar gemacht.
	Wurden Maßnahmen zur Richtlinienkontrolle ergriffen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten streng nach den Richtlinien des Verantwortlichen erfolgt?	Ja. - Grundlage hierfür sind verbindliche Auftragsverarbeitungsverträge (AVV) nach Art. 28 DS-GVO, in denen die Verantwortlichkeiten und zulässigen Verarbeitungstätigkeiten eindeutig geregelt sind. - Alle Mitarbeitenden, die personenbezogene Daten verarbeiten, sind vertraulich verpflichtet und regelmäßig zu Datenschutz- und IT-Sicherheitsrichtlinien geschult. Die Einhaltung der Datenschutz- und Sicherheitsrichtlinien wird durch interne Prüfungen inkl. Einbindung des externen DSB, Vier-Augen-Prinzip und Rollen- und Rechtekonzepte sichergestellt. - Änderungen an Verarbeitungsprozessen oder Datenflüssen erfolgen nur nach schriftlicher Freigabe oder Weisung des Verantwortlichen. anybills ISMS (Information Security Management System) überwacht fortlaufend die Umsetzung und Wirksamkeit dieser Richtlinien und sorgt für deren kontinuierliche Verbesserung.
	Wurden Maßnahmen zur Verfügbarkeits-kontrolle ergriffen, die vor zufälliger Zerstörung oder Verlust personenbezogener Daten schützen?	Ja. - Die Verarbeitung und Speicherung erfolgt ausschließlich in der Microsoft Azure-Cloud, die eine hochverfügbare, redundant ausgelegte Infrastruktur mit automatischer Lastverteilung und Failover-Mechanismen bereitstellt. - Regelmäßige, automatisierte Backups werden erstellt und georedundant gespeichert, um eine Wiederherstellung im Schadensfall sicherzustellen. - Die Backup- und Wiederherstellungsverfahren werden regelmäßig getestet und überwacht, um deren Wirksamkeit zu gewährleisten. - Der Zugriff auf Backup-Daten ist rollenbasiert beschränkt und nur autorisierten Personen erlaubt.

		- Monitoring- und Alerting-Systeme erkennen Ausfälle oder Datenintegritätsprobleme frühzeitig, sodass umgehend Gegenmaßnahmen eingeleitet werden können.
	Wurden Maßnahmen zur Einhaltung des Gebots der Datentrennung ergriffen, so dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden?	Ja. - Personenbezogene Daten verschiedener Kunden, Mandanten und Verarbeitungszwecke werden in logisch voneinander isolierten Datenbereichen (Tenant- oder Workspace-Strukturen) innerhalb der Microsoft Azure-Cloud gespeichert. - Die Trennung erfolgt über getrennte Datenbanken, Container und/oder Speicherbereiche sowie durch rollenbasierte Zugriffskontrollen. - Entwicklungs-, Test- und Produktivumgebungen sind technisch und organisatorisch strikt voneinander getrennt. - Zugriff auf Daten ist nur entsprechend des jeweiligen Zwecks und Berechtigungskontexts möglich; eine Vermischung von Daten verschiedener Kunden oder Zwecke ist systemseitig ausgeschlossen.
	Wurden Maßnahmen ergriffen, die die Wiederherstellbarkeit der Systeme im Falle einer Störung gewährleisten?	Ja. - Die gesamte Systeminfrastruktur wird in der Microsoft Azure-Cloud betrieben, die georedundante Speicherorte und automatische Failover-Mechanismen bereitstellt. - Regelmäßige, automatisierte Backups aller relevanten Systeme und Daten werden durchgeführt und in getrennten, sicheren Speicherbereichen aufbewahrt. - Disaster-Recovery- und Business-Continuity-Pläne definieren klare Verantwortlichkeiten, Wiederherstellungszeiten (RTO) und Datenwiederherstellungspunkte (RPO). - Die Wiederherstellungsverfahren werden regelmäßig getestet und dokumentiert, um ihre Wirksamkeit und Aktualität sicherzustellen. - Monitoring- und Incident-Response-Prozesse erkennen Systemstörungen frühzeitig und ermöglichen eine schnelle Reaktion und Wiederherstellung betroffener Dienste.
	Wurden Maßnahmen ergriffen, die sicherstellen, dass alle Funktionen der eingesetzten Systeme verfügbar sind und auftretende Störungen gemeldet werden?	Ja. - Die Systeme werden vollständig in der Microsoft Azure-Cloud betrieben, die eine hochverfügbare, skalierbare und überwachte Infrastruktur bereitstellt. - Ein zentrales Monitoring- und Alerting-System überwacht kontinuierlich alle kritischen Dienste, Schnittstellen und Datenflüsse. - Bei Abweichungen, Ausfällen oder Performance-Einschränkungen werden automatisierte Benachrichtigungen an das zuständige DevOps- bzw. Incident-Response-Team ausgelöst. - anybill betreibt einen standardisierten Incident-Management-Prozess, der Analyse, Eskalation, Kommunikation und Nachverfolgung aller Störungen regelt. - Regelmäßige System- und Funktions-Tests, einschließlich automatisierter Health-Checks und Lasttests, stellen die Funktionsfähigkeit und Belastbarkeit der Systeme sicher.
	Wurden Maßnahmen ergriffen, um zu verhindern,	Ja.

	dass gespeicherte personenbezogene Daten aufgrund von Störungen des Systems beschädigt werden?	- Die Datenverarbeitung und -speicherung erfolgt ausschließlich in der Microsoft Azure-Cloud, die durch redundante Speicherarchitekturen und integrierte Fehlerkorrekturmechanismen (z. B. automatische Prüfsummenvalidierung) Datenintegrität gewährleistet. - Transaktions- und Sicherungsmechanismen in den eingesetzten Datenbanken verhindern inkonsistente oder unvollständige Schreibvorgänge bei Störungen. - Regelmäßige Backups und Replikationen stellen sicher, dass Daten bei einem Ausfall oder einer Beschädigung aus einem fehlerfreien Zustand wiederhergestellt werden können. - Monitoring- und Alerting-Systeme überwachen kontinuierlich die Datenintegrität und Systemstabilität; erkannte Fehler oder Abweichungen werden automatisch gemeldet und behoben. - Die Wiederherstellungsverfahren und Datenintegritätsprüfungen werden regelmäßig getestet und dokumentiert, um ihre Wirksamkeit sicherzustellen.
	Ist ein Löschkonzept vorhanden?	Ja. anybill verfügt über ein Löschkonzept, das Bestandteil des Information Security Management Systems (ISMS) ist. Das Löschkonzept definiert auslösende Ereignisse, Löschfristen, die Art der Löschung sowie Maßnahmen zur Wirksamkeitskontrolle und stellt sicher, dass personenbezogene Daten gemäß den Grundsätzen der Datenminimierung und Speicherbegrenzung verarbeitet und fristgerecht gelöscht werden.

Versionierung

Version	**Datum**	**Änderungen**
Aktuelle Version	**10.02.2026**	**Präzisierungen in I (2), III, (1), V (4), VII (1), VII (2), Formatierung, Verbesserte Referenzierungen.**
20260126	26.01.2026	Präzisierung DVV-Regelungen, Anpassung Hauptsitz-Adresse
20260107	07.01.2026	Aktualisierung TOMs, Löschkonzept
20251027	27.10.2025	Aktualisierung TOMs
20250210	10.02.2025	Allgemeine Aktualisierungen
20240110	25.09.2024	Allgemeine Aktualisierungen
20240901	01.09.2024	Allgemeine Aktualisierungen
20231001	01.10.2023	Allgemeine Aktualisierungen