Vertrag zum Shared-Service

Die beiden Parteien

Vertragspartner aus dem Online-Vertragskonfigurator

nachfolgend **Mandantin** genannt und

debixx Gesellschaft für Debitoren- und Kundenmanagement mbH
Augustinusstraße 11a
50226 Frechen

vertreten durch die Geschäftsführer Frank Haße und Holger Ziegert,
nachfolgend **debixx** genannt, schließen folgenden Vertrag zum Shared-Service.

Präambel

Debixx betreibt für die Mandantin eine Debitoren- und Kundenverwaltung, in der sie insbesondere die in der **Anlage 1 „Leistungsbeschreibung“** Tätigkeiten erbringt. Sie agiert als Erfüllungsgehilfe der Mandantin für die Pflege von Kundendaten und Auftragsdaten, die Generierung von Forderungen aus diesen Auftragsdaten sowie deren Beibringung und Verbuchung.

Die Mandantin steht in einem direkten Auftragsverhältnis zu ihren Kunden. Das Auftragsverhältnis kann den Verkauf und den Verleih von Produkten, die Erbringung von Dienstleistungen oder die Vermietung von Flächen und Räumen beinhalten. Entsprechend des Auftragsverhältnisses schuldet der Kunde der Mandantin einmalige oder regelmäßige Entgelte (Forderungen), deren Höhe und Fälligkeiten in Rechnungen, Abonnements, Dienstleistungsverträgen oder Mietverträgen definiert sind.

Diese Vereinbarung gilt für Angebote der Mandantin in der Bundesrepublik Deutschland. Möchte die Mandantin ihr Konzept in anderen Ländern anbieten, so ist eine neue Vereinbarung zwischen der Mandantin und der debixx diesbezüglich abzuschließen.

Die Leistungen des Shared-Services sind in den **Anlagen 1 bis 4** zu diesem Vertrag detailliert beschrieben. Darüber hinaus Insoweit regeln die Mandantin und die debixx was Parteien wie folgt:

§1 Vertragslaufzeit

Dieser Vertrag tritt mit dem Online-Abschluss in Kraft. Er wird zunächst für die Basislaufzeit von 24 Monaten geschlossen und verlängert sich danach automatisch und unbefristet um jeweils 12 Monate, wenn er nicht mit einer Frist von 6 Monaten zum jeweils möglichen Vertragsende schriftlich durch einen der Vertragsparteien gekündigt wird**.**

§2 Personalqualifikation

Die debixx verpflichtet sich, für sämtliche Arbeiten im Rahmen dieses Vertrages ausschließlich geschultes und qualifiziertes Personal einzusetzen (auch externes Personal; siehe §4). Das Personal der debixx ist durch die debixx zur Einhaltung der Bestimmungen zur DSGVO (Datenschutzgrundverordnung) für den Umgang mit personenbezogenen Daten eingewiesen und verpflichtet worden.

§3 Mitwirkungspflicht der Mandantin

Die Mandantin sagt der debixx die unentgeltliche Mithilfe ihres Personals und Partner zur Erfüllung der in diesem Vertrag definierten Pflichten zu. Die Mithilfe bezieht sich auf:

- Unverzügliche und unaufgeforderte Weitergabe von neuen Auftragsverhältnissen (oder deren Kopien), Kündigungen, Ruhezeitanträgen, Atteste oder anderer für die debixx relevante Daten an die debixx über die in §1 Ziffer 2ff aufgeführten Kommunikationswege.

- Erteilung von kundenbezogenen Auskünften bzw. selbstständige und rechtzeitige Meldung von Vorgängen und Absprachen mit Kunden, Personal und Partner, die Auswirkung auf das Ergebnis der Arbeiten der debixx haben kann.

- Rechtzeitige Weitergabe jeglicher Art von kundenbezogenen Informationen an die debixx, die relevant zur Pflichterfüllung für die debixx sind oder zur Verhinderung von Zusatzaufwendungen führen.

- Sofern die Mandantin eine Datenverarbeitung auf Basis von Nutzungs-Informationen wünscht, muss sie diese über eine von debixx definierte, digitale Schnittstelle (JSON) zur Verfügung stellen. Gleiches gilt für andere dezentrale Informationen aus Dritt-Systemen, die zur Datenverarbeitung durch die debixx verwendet werden sollen. Die Anbindung von Drittsystemen werden im Rahmen von Projekten außerhalb dieser Vereinbarung definiert und umgesetzt, wenn diese möglich sind. Es entstehen in der Regel Zusatzkosten.

- Aktive Mithilfe bei Problemen und Arbeiten, die lediglich in Zusammenarbeit mit dem Personal der Mandantin wirtschaftlich sinnvoll oder zeitlich bedingt erfüllt werden können.

Die Mandantin nimmt zur Kenntnis, dass eine Datenverarbeitung der debixx nur für diejenigen Daten übernommen werden kann, welche der debixx Seitens der Mandantin zur Verfügung gestellt worden sind. Kommt die Mandantin den aufgeführten Pflichten nicht nach, kann sie keine Ansprüche gegenüber der debixx geltend machen.

§4 Einsatz von Subunternehmen

Die debixx ist berechtigt, zur Erfüllung ihrer in diesem Vertrag definierten Pflichten Subunternehmer zu beauftragen. Die debixx darf jederzeit und ohne Rücksprache mit der Mandantin Zeitarbeitsfirmen mit der Bereitstellung fachkundiger Mitarbeiter beauftragen und diese einsetzen. Subunternehmer, externe Arbeitnehmer obliegen analog zum eigenen Personal ebenfalls den Bestimmungen zur DSGVO bzw. werden dazu schriftlich verpflichtet.

§5 Gewährleistung

Die debixx übernimmt die Gewähr, dass ihre Leistungen, die vertraglich zugesicherten Eigenschaften haben und den anerkannten Regeln des Qualitätsmanagements entsprechen.

§6 Haftung / Haftungsausschluss

Die debixx haftet nicht für das von der Mandantin zur Verfügung gestellte Datenmaterial bezüglich der Richtigkeit, Lesbarkeit oder Uneindeutigkeit und der daraus ggf. fehlerhaften Bearbeitung oder Nichtbearbeitung durch die debixx. Von der Mandantin oder Partner an die debixx übermittelte Informationen, gleich in welcher Form, werden als authentisch und als zu verarbeiten angesehen. Die debixx haftet insbesondere nicht für Fehler oder fehlerhafte Systeme Dritter.

Die debixx leistet ansonsten Schadensersatz oder Ersatz vergeblicher Aufwendungen, gleich aus welchem Rechtsgrund (z.B. Pflichtverletzung, unerlaubte Handlung) nur in folgendem Umfang:

- bei Vorsatz und grober Fahrlässigkeit, auch ihrer Erfüllungsgehilfen, unbegrenzt;

- Bei fahrlässig verursachten Sach- und Vermögensschäden haftet die debixx nur bei der Verletzung einer wesentlichen Vertragspflicht, jedoch der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren und vertragstypischen Schäden; wesentliche Vertragspflichten sind solche, deren Erfüllung den Vertrag prägt und auf die der Kunde vertrauen darf.

Die gesetzliche Haftung bei Personenschäden und nach dem Produkthaftungsgesetz bleibt unberührt.

§7 Verjährung

Ansprüche der Mandantin wegen Sach- oder Rechtsmängeln verjähren innerhalb eines Jahres ab Leistungserbringung. Für sonstige Ansprüche der Mandantin aus Vertrag sowie aus einem Schuldverhältnis gilt eine Verjährungsfrist von einem Jahr ab dem gesetzlichen Verjährungsfristbeginn. Die Ansprüche verjähren spätestens mit Ablauf der gesetzlichen Höchstfristen.

Bei Vorsatz und grober Fahrlässigkeit gelten die gesetzlichen Verjährungsfristen.

§8 Preisverbindlichkeit

Die in diesem Vertrag genannten Preise und Gebühren haben eine Gültigkeit von mindestens 12 Monaten, beginnend nach Vertragsbeginn. Ab dem 13. Monat behält sich die debixx jährliche Preisänderungen in Abhängigkeit des Preisindex der Bundesrepublik Deutschland (auch Inflationsrate und tarifliche Lohn- und Gehaltsanpassungen; Quelle IHK zu Köln) vor.

Diese Preisverbindlichkeit gilt unabhängig von Staffellungen bzw. vertraglich geregelten Preismodellen, die eine Preissteigerung oder -minderung zur Folge haben.

§9 Beendigung des Vertrages

Nach Ablauf der Vertragslaufzeit bzw. nach Kündigung, wird der Zugang der Mandantin sowie seiner Partner und Mitglieder zu dem System gesperrt und es werden alle vertraglichen Leistungen eingestellt. Die Kündigung aus wichtigem Grund bleibt vorbehalten. Ein wichtiger Grund liegt insbesondere dann vor,

- wenn die Mandantin sich mit der Zahlung von mehr als zwei aufeinanderfolgende monatlicher Entgelte vollständig oder auch teilweise in Verzug befindet

oder wenn die Mandantin gegen wesentliche Vertragspflichten verstößt.

Kündigt die debixx der Mandantin das Vertragsverhältnis aus wichtigem Grund fristlos, steht ihr ein Anspruch auf pauschalierten Schadenersatz in Höhe von 75 % des Entgeltes zu, das bis zum nächsten ordentlichen Kündigungstermin zu bezahlen gewesen wäre. Die Berechnung findet auf Basis der Systemdaten zum Ersten des jeweiligen Monats, in dem die Kündigung erfolgt, statt.

Stellt die debixx ihre Leistungen unberechtigt ein, ist sie gegenüber der Mandantin zum Ersatz des der Mandantin nach dem Gesetz zustehenden Schadens verpflichtet.

Jede Kündigung, egal aus welchem Grund muss schriftlich erfolgen.

§10 Entgelte, Zahlungsbedingungen und Rechnungslegung

Die Vergütung für die in diesem Vertrag aufgeführten Dienstleistungen findet auf Basis einer monatlichen Abrechnung statt. Das Entgelt berechnet sich aus den in der **Anlage 2 „Preisliste“** zu dieser Vereinbarung aufgeführten Punkte.

Die Vergütung wird zum Letzten eines jeden Monats für den laufenden Monat erhoben und fällig. Die Vergütungspflicht beginnt mit Leistungsbeginn durch die debixx, aber frühestens mit Beginn dieser Vereinbarung. Gerät die Mandantin mit der Zahlung in Verzug, ist die debixx berechtigt, auf die fälligen monatlichen Gebühren den gesetzlichen Verzugszins zu erheben. Da die Leistung nach dem Kalender bestimmt ist, gerät die Mandantin in Verzug, ohne dass es einer separaten Mahnung durch die debixx bedarf.

Leistungen der debixx außerhalb der Leistungszeiten, sonstige Leistungen bei der Mandantin sowie sonstige gesondert zu vergütenden Leistungen werden gemäß einer gesonderten Parteivereinbarung oder nach Aufwand berechnet. Über die nach Aufwand abzurechnenden Arbeiten werden die Mitarbeiter der debixx Leistungsnachweise ausfüllen, welche nach Beendigung der Arbeiten von der Mandantin unterzeichnet werden.

Fahrtkosten und sonstige Spesen für Leistungen, welche die debixx nicht an ihrem Geschäftssitz erbringt, werden gegen Nachweis gesondert berechnet. Diese Leistungen werden jeweils zum Ende des Kalendermonates abgerechnet und mit der nächsten Monatsgebühr in Rechnung gestellt.

Alle Zahlungen sind innerhalb von 4 Tagen nach Zugang der Rechnung ohne Abzug zu leisten. Skonto wird nur bei schriftlicher Vereinbarung gewährt.

Alle in diesem Vertrag und Anlagen genannten Preise sind Nettopreise und verstehen sich zzgl. der jeweils aktuellen Umsatzsteuer in der Bundesrepublik Deutschland.

Die Zahlungen aus oben genannten Rechnungen und Einzelfakturen erfolgt monatlich mittels SEPA-Lastschriftverfahren durch die debixx selbst oder einer Ihrer Erfüllungsgehilfen (z. B. Faktoringunternehmen) ab dem 01. Werktag des Berechnungsmonats. Die Mandantin erteilt der debixx dazu eine SEPA Einzugsermächtigung (separates Formular).

§11 Erfüllungsort und Gerichtsstand

Erfüllungsort für Zahlungen und Gerichtsstand ist Köln, Deutschland. Es findet ausschließlich deutsches Recht unter Ausschluss etwaiger internationaler Regelungen Anwendung.

§12 Schlussbestimmungen

Alle Anlagen **(Anlagen 1 bis 4)** zu diesem Vertrag sind Bestandteil des Vertrages.

Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden oder sollte der Vertrag unvollständig sein, wird die Wirksamkeit des Vertrages im Übrigen nicht berührt. Die Vertragspartner werden die unwirksame Bestimmung durch eine solche Bestimmung ersetzen, welche dem Sinn und Zweck der unwirksamen Bestimmung in rechtswirksamer Weise am nächsten kommt. Dasselbe gilt für Vertragslücken.

Vertrag wird in Textform geschlossen und ist ohne Unterschrift gültig. Die Rechtsverbindlichkeit ist durch das Absenden des Online-Formulars zum Abschluss der Vereinbarung sowie durch die Bestätigung des daraus erfolgen E-Mail-Links entstanden.

Anlage 1 „Leistungsbeschreibung“

§1 System

1. EDV-System

debixx nutzt zur Erfüllung ihrer Aufgaben, gemäß diesem Vertrag unter anderem die elektronische Datenverarbeitung; Datenverarbeitungssoftware unterschiedlicher Hersteller. Die Wahl der für die Erbringung der vertraglichen Verpflichtungen einzusetzenden Programme, Tools und Netzwerk-/Datenstrukturen (z. B. Internetserver als Softwarehost und Datenspeicher) und sonstiger Technologie - im Folgenden System genannt - am Erfüllungsort steht der debixx frei.

Die Mandantin nimmt zur Kenntnis, dass die debixx ihre Dienstleistungen im Rahmen dieser Vereinbarung nur auf Basis bestimmter Systeme vollständig erbringen kann. Setzt die Mandantin nach Vertragsschluss oder während der Vertragslaufzeit ein anderes System als ein für debixx geeignetes System ein und macht der debixx hierdurch ihre Leistungserbringung (auch zu Teilen) unmöglich, so ist die debixx zur außerordentlichen, fristlosen Kündigung dieses Vertrages berechtigt.

Kann und möchte die debixx ihre Leistungen auf Basis eines anderen, von der Mandantin vorgegebenen Systems erbringen (auch teilweise), so kann die debixx einen anderen, auch höheren Preis für ihre Leistungen gemäß dieses Vertrages erheben, wenn durch die Nutzung dieses anderen Systems ein höherer Aufwand bei der debixx besteht. Können Leistungspunkte gemäß dieser Vereinbarung aufgrund des anderen Systems dauerhaft oder zeitweise durch debixx nicht mehr erbracht werden, so schuldet debixx diese Leistungen für diesen Zeitraum nicht. Der Mandantin entsteht dadurch kein Anspruch auf einen Kostenersatz oder geringeren Kosten.

2. Datenendgeräte

Am Erfüllungsort verwendet die debixx Datenendgeräte (EDV-Hardware und Telefone) zur Ausführung ihrer Tätigkeiten. Für die Mandantin fallen keine Kosten zur Anschaffung oder Reparatur dieser Datenendgeräte an. Die debixx ist frei in ihrer Wahl dieser Datenendgeräte.

Die Mandantin verpflichtet sich, auf eigene Gefahr und Rechung für die Bereitstellung geeigneter EDV-Hardware in ihrem Arbeitsumfeld und bei den Partnern zu sorgen, um der Mitwirkungspflicht ihrer Mitarbeiter und Mitarbeiterinnen und der Partner (siehe §3) nachzukommen. Diese sind je nach Anwendungsbereich mindestens ein Personalcomputer mit Dokumentenscanner oder sonstige smarte Hardware, die es erlaubt, Dokumente zu scannen und über ein Browser-Formular zu übertragen.

§2 Telefondienst für Mandantin, Kunden, Personal und Partner

2.1 Besetzung des Telefons (Erreichbarkeit)

Die Kundenverwaltung des Shared-Service ist für die Mandantin, Kunden, Personal und Partner. Sie ist von Montag bis Freitag (außer an gesetzlichen Feiertagen im Bundesland NRW sowie am 24. Dezember sowie am 31. Dezember; nachfolgend gilt die Definition als „Werktag“) jeweils von 09:00 bis 12:00 Uhr und von 14:00 Uhr bis 17:00 Uhr besetzt.

2.2 Verwaltung für Kunden

a) Die Kommunikation bezüglich der Verwaltung für die Kunden erfolgt über eine Festnetznummer der debixx. Die debixx verpflichtet sich, dafür Sorge zu tragen, dass die Anrufer direkt bzw. in einem angemessenen Zeitraum angenommen werden. Für die Kunden anfallende Kosten zur Anwahl der Festnetznummer werden von der debixx nicht erstattet.

Weitere Kommunikationsmöglichkeiten für Kunden sind Briefe, eMails sowie elektronische Kontaktformulare, die debixx der Mandantin für ihre Homepage bereitstellt.

Briefe, Zustellungen von Einschreibesendungen und Dokumenten sind an ein Postfach der Mitgliederverwaltung zu richten. Das Postfach wird von der debixx an Werktagen täglich geleert.

Telefonate, Briefe oder eMails, aus denen eine Datenverarbeitung hervor geht, wird im EDV-System kundenspezifisch zwecks Nachvollziehbarkeit von dem sachbearbeitenden Personal der debixx protokolliert und bearbeitet.

b) Wenn es für die Bearbeitung einer Sache notwendig ist, wird ein Mitglied ebenfalls telefonisch, per Brief oder eMails kontaktiert.

2.3 Shared-Service für Personal der Mandantin und der Partner

Die Kommunikation mit dem Personal der Mandantin und der Partner erfolgt analog zu Punkt 1.2. „Verwaltung für Kunden“. Sie erhalten ggf. eine abweichende Telefonnummer.

§3 Bürotätigkeiten

Die Mandantin nutzt zur Übermittlung von Unterlagen, die durch die debixx bearbeitet werden sollen, die im Vertrag zum Shared-Service definierten Kommunikationswege. Die debixx erfasst und ändert die Daten Mitglieder sowie deren Vertragsdaten im System.

Eine Zusendung von Papier-Dokumenten als Grundlage zur Datenerfassung ist ausgeschlossen. Die Datenvorlage muss in allen Fällen alle relevanten Daten leserlich und korrekt enthalten. Die Mandantin verpflichtet sich sicherzustellen, dass in der Organisation der Mandantin die zur Änderung von Daten autorisierten Mitarbeiter der debixx immer aktuell bekannt sind.

3.1 Erfassung von Stammdaten und Vertragsdaten

Die debixx erfasst nach Auftrag folgende Daten:

a)
- Adressdaten der Firma, des Kunden oder des Partners (Vertragspartner / Vertragsnutzer)
- Weitere relevante Daten zu Personen oder Firmen (zu definieren)
- Bankverbindung des Rechnungs- oder Gutschriftempfängers

b)
- Vertragskonditionen wie:

  Bei Einzelfaktura:
  - Rechnungsnummer
  - Rechnungsbetrag
  - Rechnungsdatum
  - Rechnungsfälligkeit
  - Ggf. Ratenzahlungsvereinbarungen

  Bei Dauerschuldverhältnissen
  - Vertragsbeginn
  - Vertragslaufzeit
  - Vertragsverlängerung
  - Forderungen mit entsprechender Zahlweise (Art und Zyklus)
  - Sonderforderungen und Gebühren (Art und Zyklus)

Die Verträge werden derart erfasst, dass ein elektronischer Lastschriftenlauf mittels des verwendeten Systems möglich ist, insofern Punkt 2.1 a) erfüllt ist.

3.2 Pflege von Stammdaten

Die unter §2 Ziffer 2.1 a) genannten Stammdaten werden nach Bedarf gepflegt. Die Pflege von Stammdaten ist bedingt durch:

- Aufforderung durch Personal der Mandantin (Auftragsdatenverarbeitung)
- Aufforderung durch den Kunden selbst, wenn die Mandantin dem grundsätzlich zustimmt
- Informationen aus Auskunftssystemen wie Schufa oder Inkassobüro

3.3 Pflege von Rechnungs- und Vertragsdaten

Die unter §2 Ziffer 2.1 b) genannten Rechnungs- und Vertragsdaten werden nach Bedarf gepflegt. Ebenso werden bei Dauerschuldverhältnissen Ruhe-/Gratiszeiten sowie Kündigungen erfasst. Die Pflege von Rechnungs- und Vertragsdaten ist bedingt durch:

- Aufforderung durch Personal der Mandantin (Auftragsdatenverarbeitung)
- Aufforderung durch den Kunden selbst, wenn die Mandantin dem grundsätzlich zustimmt

Die debixx hält sich aufgrund ansonsten zu hoher Arbeitsaufwendungen, die durch häufige Rückfragen mit dem Personal der Mandantin beiderseits entstehen würden, Entscheidungen hinsichtlich der Akzeptanz von Gründen für Nutzungspausen und Minderungen (z. B. bei unklarer Sachlage oder Kulanz) aus eigenem Ermessen und im Sinne der Mandantin vor.

Die von den Kunden an die debixx gerichteten Schreiben, zugestellten Schriftstücke sowie Dokumente (z. B. Kündigungen von Verträgen etc.) sind als rechtsverbindliche Zustellung an den Vertragspartner (Mandantin), anzusehen und zu behandeln.

Die debixx richtet sich im Allgemeinen bei der Pflege und Prüfung auf Rechtsmäßigkeit erhaltener Anträge auf z. B. Nutzungspausen und Kündigungen (insbesondere bei vorzeitigen Kündigungen) nach aktuellen Rechtsprechungen. Grundlegende Vorgaben zur Akzeptanz von Anträgen und Kündigungen gibt die Mandantin vor.

3.4 Fristen für die Erfassung und Pflege von Kunden-Stammdaten, Rechnungs- und Vertragsdaten

Die debixx gewährleistet die Erfassung und Pflege von Stamm-, Rechnungs- und Vertragsdaten binnen 4 Werktagen nach Erhalt entsprechender Schriftstücke durch die Mandantin, die Firma, der Kunde oder den Partner. Wird das Schriftstück vor 10:00 Uhr eines Werktages erhalten, so zählt dieser als erster Werktag für diese Frist. Ab 10:00 Uhr zählt der folgende Werktag als erster Werktag im obigen Sinn. Ausnahme besteht, wenn der debixx mehr als 50 Schriftstücke pro Tag oder Wochenende eingereicht werden. Dann kann sich die Verarbeitungszeit auf 5 Werktage erhöhen.

§4 Debitorenmanagement

4.1 Erstellung von Forderungslisten

Die debixx generiert zu den von der Mandantin genannten Stichtagen Forderungslisten zu Forderungen, Sonderforderungen und -gebühren seiner Kunden unabhängig der Zahlarten der Kunden (Barzahler, Überweiser und Lastschriftler). Diese Forderungslisten (speziell die der Lastschriftler) dienen der Beitragserhebung, der Erhebung von Sonderforderungen und Gebühren.

Die Listen werden an Werktagen stichtagsgenau erstellt. Falls der Stichtag auf einen Nichtwerktag fällt, werden die Listen am nächst folgenden Werktag rückwirkend zum Stichtag erstellt. Ausnahmen definiert die debixx zusammen mit der Mandantin.

Die Forderungslisten basieren auf dem Datenbestand, der bis zu diesem Zeitpunkt in der EDV erfasst ist also maximal mit einem zeitlichen Verzug wie unter §2 Ziffer 2.4 definiert. Bis hin zum 4. bzw. 5. Werktag nach dem Stichtag sind somit ggf. Korrekturen der Forderungslisten möglich.

Die für die Forderungslisten relevanten Daten, die aber ggf. nach einem Stichtag eingepflegt werden, sind:

- Stundungen und Minderungen, die kurzfristig bei debixx eingehen
- Ratenkalender, die kurzfristig bei debixx eingehen
- Geänderte Bankverbindungen, die kurzfristig bei debixx eingehen
- Nutzungspausen, die kurzfristig bei debixx eingehen
- Neuverträge, die kurzfristig bei debixx eingehen
- Widersprochene Einzugsermächtigungen, die kurzfristig bei debixx eingehen

Fehlbuchungen, die auf diesen Punkten basieren obliegen nicht dem Verantwortungsbereich der debixx.

4.2 Erstellung von digitalen Lastschriftdateien zum Zahlungsverkehr

Parallel zur Erstellung der unter §3 Ziffer 3.1 beschriebenen Forderungslisten wird zeitgleich eine Datei zum elektronischen Lastschriftverfahren (SEPA) generiert. Diese Datei beinhaltet alle zur Zahlung fälligen Positionen der Zahler/Schuldner zum Stichtag, die für das Lastschriftverfahren freigegeben sind.

4.3 Ausführen von digitalen Lastschriften

debixx führt die unter Punkt 3.2 erstellen Lastschriftendateien auf Wunsch der Mandantin aus. Dazu stellt die Mandantin der debixx einen Onlinebanking-EBICS-Zugang auf das entsprechende Konto zur Verfügung. Das Konto läuft auf den Namen der Mandantin. Eine Person der debixx ist überdies Konto-Mitinhaber und ist somit zur Ausführung von digitalen Lastschriftenläufen berechtigt.

Soll debixx treuhänderisch oder im Bereich Inkasso Zahlungseinzüge vornehmen, so können Einzüge auch auf das Konto der debixx durchgeführt werden, wenn ggf. notwendige Sicherheiten durch die Mandantin bestellt sind. Dies bedingt weiterer Verabredungen zwischen der debixx und der Mandantin außerhalb dieses Vertrages.

4.4 Abarbeiten von Rückläufern aus dem digitalen Lastschriftenlauf

Die Mandantin stellt der debixx digitale Medien (vorzugsweise elektronische Kontoauszüge) oder einen direkten Kontozugang zur Verfügung, anhand derer die debixx Rückläufer aus Lastschriften ersehen und in die EDV automatisiert übertragen kann.

Entsteht bei der debixx ein Mehraufwand deshalb, weil die Mandantin die Rückläuferinformationen offline bzw. in einem nicht automatisch zu verarbeitendem Format zur Verfügung stellt, ist debixx berechtigt die Kosten für diesen Leistungspunkt entsprechend zu erhöhen.

4.5 Abarbeiten und Erfassung von Zahlungen aus Vertragsforderungen

Die Mandantin stellt der debixx digitale Medien (vorzugsweise elektronische Kontoauszüge) oder einen direkten Kontozugang zur Verfügung, anhand derer die debixx Überweisungen von Kunden aus Vertragsforderungen ersehen und in die EDV automatisiert oder manuell übertragen kann.

Die Übertragung von Zahlungseingängen bzw. Zahlungen in die EDV, die das Mitglied an Dritte leistet (z. B. externes Fakturierungsunternehmen oder Inkassounternehmen) oder auf Konten der Mandantin, zu denen debixx keinen in oben genannter Form Zugriff hat, sind aus dieser Regelung explizit ausgeschlossen.

4.6 Nachhalten von Forderungen / Erstellung von Mahnlisten

Die debixx erstellt zyklisch nach Abstimmung mit der Mandantin Listen offener Forderungen und Mahnlisten. Die Mahnlisten beinhalten stichtagsgenau den Stand mitgliedsbezogener und nach Mitglied sortierter, offener Positionen inkl. Mahnstufe und Überfälligkeitsangabe.

4.7 Durchführung von Mahnaktionen

Parallel zur Erstellung der unter §3 Ziffer 3.4 beschriebenen Mahnlisten, werden Mahnschreiben an die Mitglieder erstellt und versendet. Mahntexte, Mahnzyklen sowie Mahnkosten (Bankgebühr/Bearbeitungsgebühr) werden zwischen der Mandantin und der debixx abgestimmt.

Der Versand der Mahnschreiben wird durch die debixx durchgeführt.

Forderungsdaten bleiben bei diesem Prozess stets Eigentum der Mandantin. Mahngebühren gehören der Mandantin.

4.8 Übergabe an Inkasso oder Durchführung von Inkasso bzw. Forderungskauf

Die debixx generiert nach Vorgabe bestimmter Kriterien der Mandantin monatliche Inkassolisten, d. h. Listen, in denen Kunden nach einem erfolglosen Mahnwesen aufgeführt sind. Die debixx übernimmt nach Auftrag der Mandantin diese Inkassodaten (beinhalten Adress-, und Vertragsdaten der Mitglieder sowie ausstehende Zahlungen mit Altersangabe der Forderung. Zusätzlich alle Informationen über bereits erfolgte Mahnaktionen) in ihr Inkasso oder unterbreitet der Mandantin ein Angebot zum Kauf notleidender Forderungen.

4.9 Kostenersatz

Sollte die Mandantin Aufgaben aus dieser Vereinbarung an Dritte übergeben, so entsteht der Mandantin in keinem Fall eine finanzielle Entlastung aus dieser Vereinbarung und dieser Leistungsbeschreibung. Durch Involvierung Dritter in den beschriebenen Leistungen entstehen i. d. R. sogar Mehraufwände bei der debixx, die die debixx entsprechend an die Mandantin fakturieren darf.

§5 Administrative Richtlinien

Im Detail werden folgende Arbeitsweisen / Umsetzungen festgelegt.
Folgende administrative Richtlinien gelten als vereinbart („*“=obligatorisch):

Allgemeine Einstellung (Angaben ohne „*“ werden im Boarding angepasst):

Nr.	Einstellung	Trifft zu
1.	Debixx erhält einen EBICS-Kontozugang	Dynamisch – R&A wir separat definiert
2.	AGB der Mandantin liegen vor – Entnahme grundlegender Handlungsweisen	Dynamisch – R&A wir separat definiert
3.	Zahlart SEPA-Lastschrift ist möglich	Dynamisch – R&A wir separat definiert
4.	Zahlart Überweisung ist möglich	Dynamisch – R&A wir separat definiert
5.	Zahlart in Bar an die Mandantin ist möglich	Dynamisch – R&A wir separat definiert
6.	Zahlart EC ist möglich	Dynamisch – R&A wir separat definiert
7.	Zahlart über Dritte Zahlungsanbieter sind möglich	Dynamisch – R&A wir separat definiert
8.	Ratenzahlungen sind möglich	Dynamisch – R&A wir separat definiert
9.	Es werden Abo-Modelle abgebildet	Dynamisch – R&A wir separat definiert
10.	Es wird Einzelfaktura abgebildet	Dynamisch – R&A wir separat definiert
11.	Verträge mit Minderjährigen sind möglich	Dynamisch – R&A wir separat definiert
12.	Neuverträge mit Personen oder Firmen nach Inkasso sind möglich	Dynamisch – R&A wir separat definiert
13.	Kündigungen müssen der Schriftform genügen	Dynamisch – R&A wir separat definiert
14.	Kündigungen müssen mind. der Textform entsprechen	Dynamisch – R&A wir separat definiert
15.	Änderungen der Personen- und Bankdaten müssen der Schriftform entsprechen	Dynamisch – R&A wir separat definiert
16.	Änderungen der Personen- und Bankdaten müssen mind. der Textform entsprechen	Dynamisch – R&A wir separat definiert
17.	Änderungen der Einzugsermächtigung muss der Schriftform entsprechen	Dynamisch – R&A wir separat definiert
18.	Änderungen der Einzugsermächtigung muss mind. der Textform entsprechen	Dynamisch – R&A wir separat definiert

Verträge:

Nr.	Einstellung	Trifft zu
1.	Daten des Vertragspartners müssen vollständig vorliegen.	Dynamisch – R&A wir separat definiert
2.	Daten zur Abwicklung des Zahlprozesses müssen vollständig vorliegen; insbesondere Kontoinhaber und IBAN, wenn das SEPA-Lastschriftverfahren genutzt werden soll.	Dynamisch – R&A wir separat definiert
3.	Vertragsbeginn ist nach Abschluss immer der 1. Des Folgemonats und Vornutzung wird anteilig berechnet.	Dynamisch – R&A wir separat definiert
4.	Vertragsbeginn ist stichtagsgenau bei Vertragsabschluss.	Dynamisch – R&A wir separat definiert
5.	Vertragsdaten wie Abschluss, Vertragsbezeichnung, Beginn, Laufzeit, Fristen zur Kündigung (Erstlaufzeit und Folgelaufzeiten) und Verlängerungen sowie einmalige und regelmäßige Entgelte und Gebühren (inkl. Zyklusangabe) gehen aus der übermittelten Vereinbarung hervor.	Dynamisch – R&A wir separat definiert
6.	Papierverträge beinhalten grundsätzlich die Unterschrift eines Mitarbeiters der Kundin.	Dynamisch – R&A wir separat definiert
7.	Der Kunde muss mindestens 18 Jahre alt sein.	Dynamisch – R&A wir separat definiert
8.	Der Kunde muss mindestens 16 Jahre alt sein und der Vertrag muss zusätzlich von einem Erziehungsberechtigten unterzeichnet sein.	Dynamisch – R&A wir separat definiert
9.	Dem Kunden wird ein Zutrittsmedium ausgehändigt.	Dynamisch – R&A wir separat definiert
10.	Das Zutrittsmedium ist kostenpflichtig.	Dynamisch – R&A wir separat definiert
11.	Bei Verlust des Zutrittmediums fallen Kosten an.	Dynamisch – R&A wir separat definiert
12.	Abweichende Kontoinhaber sind erlaubt (ungleich Vertragspartner)	Dynamisch – R&A wir separat definiert

Wiedereinstieg, Übernahmen und Anpassungen bei Verträgen *:

Nr.	Einstellung	Trifft zu
1	Kunden können nach Beendigung eines Vertrages, der aufgrund von Inkasso beendet wurde, einen neuen Vertrag abschließen.	Dynamisch – R&A wir separat definiert
2	Vertragsübernahmen sind jederzeit möglich.	Dynamisch – R&A wir separat definiert
3	Vertragsanpassungen sind nur mit einem vollständig neuen Vertragsabschluss mit neuer Laufzeit möglich.	Dynamisch – R&A wir separat definiert
4	Vertragsanpassungen sind zum Ende eines Forderungszyklus jederzeit möglich.	Dynamisch – R&A wir separat definiert
5	Vertragsanpassungen sind nur zum Ende der jeweiligen Vertragslaufzeit möglich.	Dynamisch – R&A wir separat definiert
6	Vertragsanpassungen sind nur möglich, wenn diese gleich oder höherwertig sind.	Dynamisch – R&A wir separat definiert
7	Vertragsanpassungen sind kostenpflichtig.	Dynamisch – R&A wir separat definiert

Nutzungspausen *:

Nr.	Einstellung	Trifft zu
1	Eine Nutzungspause gewünscht durch den Kunden ist möglich, wenn der Nutzungsgegenstand vorübergehend nicht mehr nutzbar ist oder die Vertraglichen Leistungen vorübergehend nicht mehr erbracht werden können.	Dynamisch – R&A wir separat definiert
2	Eine Nutzungspause gewünscht durch den Kunden ist möglich, wenn dieser persönlich und mit Nachweis vorübergehend nicht mehr in der Lage ist oder es für ihn durch veränderte Umstände vorübergehend unzumutbar ist, den Nutzungsgegenstand zu nutzen oder die vertraglichen Leistungen in Anspruch zu nehmen.	Dynamisch – R&A wir separat definiert
3	Nutzungspausen haben eine zeitliche Begrenzung pro Laufzeit.	Dynamisch – R&A wir separat definiert
4	Nutzungspausen haben eine Mindestdauer.	Dynamisch – R&A wir separat definiert
5	Nutzungspausen sind kostenpflichtig (Einmalige Gebühr).	Dynamisch – R&A wir separat definiert
6	Der Vertrag verlängert sich um die Dauer der Nutzungspause.	Dynamisch – R&A wir separat definiert

Gratisnutzungen *:

Nr.	Einstellung	Trifft zu
1	Gratisnutzungen oder Minderungen von Entgelten und Gebühren können aufgrund von Kulanz, Wiedergutmachung oder berechtigten Mängeln gegeben werden.	Dynamisch – R&A wir separat definiert

Sonderkündigung *:

Nr.	Einstellung	Trifft zu
1	Eine vorzeitige Vertragskündigung durch den Kunden ist möglich, wenn der Nutzungsgegenstand nicht mehr nutzbar ist oder die Vertraglichen Leistungen nicht mehr erbracht werden können.	Dynamisch – R&A wir separat definiert
2	Eine vorzeitige Vertragskündigung durch den Kunden ist möglich, wenn dieser persönlich und mit Nachweis nicht mehr in der Lage ist oder es für ihn durch veränderte Umstände unzumutbar ist, den Nutzungsgegenstand zu nutzen oder die vertraglichen Leistungen in Anspruch zu nehmen.	Dynamisch – R&A wir separat definiert

Lastschriftläufe *:

Nr.	Einstellung	Trifft zu
1	Forderungen, die per Zahlart SEPA-Lastschrift eingezogen werden sollen, werden im Rahmen von Lastschriftläufen binnen 2 Werktagen nach Fälligkeit eingezogen.	Dynamisch – R&A wir separat definiert
2	Forderungen, die per Zahlart SEPA-Lastschrift eingezogen werden sollen, werden im Rahmen von Lastschriftläufen zum Stichtag 1. des Monats und 15. des Monats eingezogen. Es werden alle Fälligkeiten vor einem Stichtag berücksichtigt. Die Läufe werden 3 Werktage vor dem Stichtag durchgeführt, damit die Abbuchung zum Stichtag erfolgt (SEPA-Vorankündigung).	Dynamisch – R&A wir separat definiert

Rücklastschriften (RüLa) und Widerspruch bei der Zahlart SEPA-Lastschrift*:

Nr.	Einstellung	Trifft zu
1	Nach einer RLS erfolgt das erste Mahnschreiben (siehe Mahnläufe) mit der Information, dass erneut versucht wird, den Geldbetrag inkl. entstandener Bankgebühren und einer Mahngebühr abzubuchen. Erst bei einer 2. RLS wird das Einzugsverfahren gestoppt.	Dynamisch – R&A wir separat definiert
2	Nach einem Widerspruch zu einer Abbuchung erfolgt das erste Mahnschreiben (siehe Mahnläufe) mit der Information, dass nicht erneut versucht wird, den Geldbetrag inkl. entstandener Bankgebühren und einer Mahngebühr abzubuchen, da mit einem Widerspruch gleichzeitig das Mandat zur Abbuchung erlischt.	Dynamisch – R&A wir separat definiert

Mahnläufe*:

Nr.	Einstellung	Trifft zu
1	Es werden 2 kfm. Mahnungen nach einem Zahlungsverzug an den Schuldner versendet. Die Mahnzyklen bestimmt die Debixx, erfolgen aber zeitnah nach dem Zahlungsverzug und die Zahlfrist bis zum 2. Schreiben ermöglicht dem Schuldner eine Zahlung zum jeweils genannten Stichtag.	Dynamisch – R&A wir separat definiert
2	Die Mahnschreiben beinhalten neben den Vertragsforderungen und Bankgebühren auch eine Mahngebühr, die geltenden Regelungen und Rechtsprechungen entspricht.	Dynamisch – R&A wir separat definiert
3	Der Schuldner kann Zahlungsrückstände in Form einer Ratenzahlung ausgleichen. Die minimale Ratenhöhe beträgt 25% der Schuld pro Monat.	Dynamisch – R&A wir separat definiert
4	Zahlungen werden immer zunächst gegen Nebenforderungen gebucht und zwar erstens Mahngebühren und zweitens die vertraglichen Forderungen nebst Kostenaufwand wie Bankgebühren, die durch den Schuldner verursacht wurden.	Dynamisch – R&A wir separat definiert

Inkasso*:

Forderungen aus einem Dauerschuldverhältnis

Nr.	Einstellung	Trifft zu
1	Nicht vollständig ausgeglichene Forderungen gelangen nach der letzten kfm. Zahlungsfrist automatisch in das Einzugs-Inkasso der Debixx.	Dynamisch – R&A wir separat definiert
2	Vor der Übergabe erhält die Mandantin eine Freigabeliste für diese Fälle und nur freigegebene Forderungen gelangen in das Inkasso der Debixx.	Dynamisch – R&A wir separat definiert
3	Es gibt in den AGB eine Vorfälligkeitsklausel für Forderungen in der Zukunft. Mit Abgabe in das Inkasso werden alle künftigen Forderungen fällig.	Dynamisch – R&A wir separat definiert
4	Mit Abgabe in das Inkasso wird der Vertrag zwischen der Mandantin und dem Schuldner im Rahmen der Schadenminderungspflicht zum nächstmöglichen Zeitpunkt gekündigt.	Dynamisch – R&A wir separat definiert
5	Im Rahmen des Einzug-Inkassos werden 2 Inkassoschreiben an den Schuldner versendet, die neben den Vertragsforderungen sowie Mahn- und Bankgebühren auch eine Inkassogebühr der Debixx nach gültiger Gebührenverordnung enthält.	Dynamisch – R&A wir separat definiert
6	Zahlungen werden immer zunächst gegen Nebenforderungen gebucht und zwar erstens Inkassogebühr, zweitens Mahngebühren und drittens die vertraglichen Forderungen nebst Kostenaufwand wie Bankgebühren, die durch den Schuldner verursacht wurden.	Dynamisch – R&A wir separat definiert
7	Nicht vollständig ausgeglichene Forderungen gelangen nach der letzten Inkasso-Zahlungsfrist automatisch in den Forderungskauf. Dabei macht die Debixx der Mandantin ein Angebot zum Ankauf der bestehenden Forderungen zu einem jeweiligen Kunden (Siehe Inkasso-Vereinbarung).	Dynamisch – R&A wir separat definiert

Forderungen aus einer Einzelfaktur

Nr.	Einstellung	Trifft zu
1	Nicht vollständig ausgeglichene Forderungen gelangen nach der letzten kfm. Zahlungsfrist automatisch in das Einzugs-Inkasso der Debixx.	Dynamisch – R&A wir separat definiert
2	Vor der Übergabe erhält die Mandantin eine Freigabeliste für diese Fälle und nur freigegebene Forderungen gelangen in das Inkasso der Debixx.	Dynamisch – R&A wir separat definiert
3	Im Rahmen des Einzug-Inkassos werden 2 Inkassoschreiben an den Schuldner versendet, die neben den Vertragsforderungen sowie Mahn- und Bankgebühren auch eine Inkassogebühr der Debixx nach gültiger Gebührenverordnung enthält.	Dynamisch – R&A wir separat definiert
4	Zahlungen werden immer zunächst gegen Nebenforderungen gebucht und zwar erstens Inkassogebühr, zweitens Mahngebühren und drittens die vertraglichen Forderungen (Rechnungsbetrag) nebst Kostenaufwand wie Bankgebühren, die durch den Schuldner verursacht wurden.	Dynamisch – R&A wir separat definiert
5	Nicht vollständig ausgeglichene Forderungen gelangen nach der letzten Inkasso-Zahlungsfrist automatisch in den Forderungskauf. Dabei macht die Debixx der Mandantin ein Angebot zum Ankauf der bestehenden Forderungen zu einem jeweiligen Kunden (Siehe Inkasso-Vereinbarung).	Dynamisch – R&A wir separat definiert

Besonderheiten *:

Nr.	Einstellung	Trifft zu
1	Rückerstattungen von Geldern werden der Mandantin weiter geleitet.	Dynamisch – R&A wir separat definiert
2	Überzahlungen werden mit kommenden Forderungen verbucht, wenn möglich.	Dynamisch – R&A wir separat definiert
3	Unterzahlungen werden mit den ältesten Forderungen verrechnet.	Dynamisch – R&A wir separat definiert

Anlage 2 „Preisliste“

Folgende Preisliste gilt als vereinbart:

Dienstleistung

Nr.	Kostenart	Preis	Zyklus und Stichtag
1	Dienstleistungsgebühr für Kunden im Dauerschuldverhältnis	3,9 % der Netto-Zahlungseingänge im Leistungsmonat (bezogen auf alle Vertragsforderungen und ohne Gebühren)	monatlich zum Ende des Leistungsmonats
3	Setup-Gebühr zur Dienstleistung	2.997,00 Euro	einmalig
4	Sonderleistungen im Bereich Bürotätigkeiten (fallen nur in Abstimmung und separater Beauftragung an)	60,00 Euro + Material nach Aufwand	pro Stunde zum Ende des Leistungsmonats
5	Briefversand (alle Varianten)	1,10	pro Versand (zzgl. Porto) zum Ende des Leistungsmonats
6	Mahngebühren	Pro Mahnschreiben stellen wir 50% der Mahngebühren in Rechnung	Monatlich zum Ende des Leistungsmonats

Anlage 3 „Auftragsverarbeitung nach Art. 28 DS-GVO“

Die Parteien stehen im Rahmen der geschlossenen, vertraglichen Vereinbarungen in einem direkten Auftragsverhältnis. Bei der Erbringung der vertraglich geschuldeten Leistungen verarbeitet und speichert debixx im Auftrag der Mandantin personenbezogene Daten. Daher ist es erforderlich, die datenschutzrechtlichen Verpflichtungen mittels einer Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO niederzulegen. Die Vereinbarung gilt für alle Tätigkeiten, bei denen Mitarbeiter der debixx oder durch sie beauftragte Dritte mit personenbezogenen Daten der Mandantin umgehen können.

§ 1 Gegenstand und Dauer des Auftrags

a. Gegenstand der Vereinbarung ist die Verarbeitung (Vgl. Art. 4 Nr. 2 DS-GVO) von Kunden- und Mitgliederdaten der Mandantin mittels einer Online-Verwaltungssoftware.

b. Die Dauer dieser Vereinbarung ergibt sich aus der jeweiligen Dauer der Beauftragungen durch die Mandantin.

§ 2 Auftragsinhalt

a. Art und Zweck der Verarbeitung personenbezogener Daten durch debixx für die Mandantin ergeben sich aus dieser Vereinbarung.

b. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/- kategorien:
- Personenstammdaten, Kontaktdaten wie z.B. Adresse, Telefonnummer, E-Mail-Adresse,
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse),
- Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten,
- Gesundheitsdaten (Atteste), Kontaktbemerkungen,
- Bewegungsdaten, wie Check-In, Teilnahmen an Event und Besuche,
- Zahlungsdaten inkl. Bankdaten und Zahlungsverläufen,
- Planungs-, Steuerungs- und Protokolldaten.

c. Die Kategorien der durch die Verarbeitung betroffenen Personen sind:
- Interessenten
- Kunden
- Mitarbeiter
- Lieferanten
- Ansprechpartner

d. Die Datenverarbeitung erfolgt zu dem Zweck der Unterstützung der Mandantin bei der Anbahnung, dem Abschluss und der Erfüllung von Nutzungsverträgen für Dienstleistungen und Räumen einschließlich der Kontaktaufnahme per E-Mail, Telefon oder Post für Werbemaßnahmen im Rahmen der Anbahnung, bei bestehenden Nutzungsverträgen oder Werbemaßnahmen nach beendeten Nutzungsverträgen. Die Daten können zum Ankauf und Einzug von Forderungen verarbeitet werden, wenn diese fällig oder überfällig sind. Die Datenverarbeitung erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung der Mandantin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 3 Technische und organisatorische Maßnahmen

a. debixx hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen (im Folgenden: TOMs) vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und der Mandantin zur Prüfung zu übergeben. Wenn die Mandantin die TOMs akzeptiert, werden diese Grundlage des Auftrags. Soweit die Prüfung/ein Audit der Mandantin einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

b. debixx hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um solche der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (siehe Anlage TOMs).

c. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es debixx gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert.

d. Die Mandantin verpflichtet sich, die TOMs der debixx - Anlage - geheim zu halten - sie insbesondere nicht Dritten zugänglich zu machen. Eine Weitergabe ist der Mandantin lediglich im Rahmen der Ausübung ihrer Kontrollrechte nach § 7 dieser Vereinbarung gestattet.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

a. debixx darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Mandantin berichtigen, löschen oder deren Verarbeitung einschränken (Art. 16-19 DS-GVO). Soweit eine betroffene Person sich diesbezüglich unmittelbar an debixx wendet, wird debixx dieses Ersuchen unverzüglich der Mandantin weiterleiten und sie bei der Bereitstellung jener Informationen unterstützen, vorausgesetzt:

1. die Mandantin hat debixx dazu schriftlich aufgefordert und
2. die Mandantin erstattet debixx die durch diese Unterstützung entstandenen Kosten.

b. Soweit vom Leistungsumfang umfasst, sind das Löschkonzept einschließlich seiner Umsetzung, die Rechte auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der Mandantin unmittelbar durch debixx sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten der debixx

debixx hat zusätzlich zur Einhaltung der Bestimmungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO. debixx gewährleistet insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Datenschutzbeauftragte(r) bei der debixx ist in §6 „Unterauftragsverhältnisse“ aufgeführt. Ein Wechsel des Datenschutzbeauftragten wird der Mandantin unverzüglich mitgeteilt.

b) Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO debixx setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit der Daten verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. debixx und jede debixx unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend den Weisungen der Mandantin verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen TOMs gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (siehe Anlage TOMs).

d) Unverzügliche Information der debixx durch die Mandantin über bei ihr eingegangene Beschwerden und/oder Anfragen von betroffenen Personen, insbesondere Auskunftsersuchen gemäß Art. 15 DS-GVO und die Geltendmachung von Betroffenenrechten nach Art. 16 ff DS-GVO.

e) Zusammenarbeit der Mandantin und debixx mit der Aufsichtsbehörde auf Anfrage bei der Erfüllung ihrer Aufgaben.

f) Die unverzügliche Information der Mandantin über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei debixx ermittelt oder wenn die Daten der Mandantin bei debixx durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden. debixx wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten bei der Mandantin liegt.

g) Soweit die Mandantin einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeiten- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei debixx ausgesetzt ist, hat sie debixx nach besten Kräften zu unterstützen. Die Mandantin erstattet debixx die durch diese Unterstützung entstandenen Kosten.

h) debixx kontrolliert regelmäßig die internen Prozesse sowie die TOM´s um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist.

i) Nachweisbarkeit der getroffenen TOMs gegenüber der Mandantin im Rahmen ihrer Kontrollbefugnisse nach § 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

a. Als Unterauftragsverhältnisse im Sinne dieser Bestimmung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Nicht hierzu gehören Nebenleistungen, die debixx 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. debixx ist jedoch verpflichtet, zur

Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Mandantin auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

b. Debixx darf Unterauftragnehmer (weitere Auftragsverarbeiter) grundsätzlich nur nach vorheriger, ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung der Mandantin beauftragen.

Ohne schriftliche Zustimmung kann debixx zur Vertragsdurchführung unter Wahrung ihrer unter § 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen im Sinne des § 15 AktG einsetzen, wenn sie dies der Mandantin vor Beginn der Verarbeitung oder Nutzung mitteilt.

Die Mandantin stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Nr.	Unterauftragnehmerin	Erreichbarkeit	Leitung
1.	Inkasso Becker Wuppertal GmbH & Co KG	Friedrich-Engels-Allee 32 42103 Wuppertal www.inkassobecker.de	Datenverarbeitung bei Ankauf notleidender Forderungen
2.	Rechtsanwalt Torsten Kowalewsky	Stapelkai 50735 Köln www.kowalex.de	Dateneinsicht und -speicherung bei Inkasso-Mandaten
3.	Rechtsanwältin Dr. Sarah Nemes	Herzogstraße 22-24 50667 Köln www.nickel-nemes.de	Datenschutzbeauftragte
4.	Zendesk GmbH	Neue Schönhauser Str. 3-5 10178 Berlin www.zendesk.de	Datenspeicherung im Rahmen des Ticket-System
5.	HETZNER Online GmbH	Industriestraße 25 91710 Gunzenhausen www.hetzner.com	Provider - Datenverarbeitung bei Speicherung von Daten auf Servern der Unterauftragnehmerin
6.	Condimar GmbH	Menzelstraße 11 50169 Kerpen www.condimar.com	Software-System - Datenverarbeitung bei Speicherung von Daten auf Servern der Unterauftragnehmerin

c. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

1. debixx eine solche Auslagerung auf Unterauftragnehmer der Mandantin eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

2. die Mandantin nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber debixx schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

3. eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

d. Die Weitergabe personenbezogener Daten der Mandantin an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

e. Es werden nur Unterauftragnehmer ausgewählt, die die vereinbarten Leistungen innerhalb der EU/des EWR erbringen.

f. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung der Verantwortlichen und ggf. der debixx (mind. Textform); allen weiteren Unterauftragnehmer der Vertragskette sind inhaltlich die gleichen vertraglichen Regelungen aufzuerlegen.

g. Bei Mängeln in der Datenverarbeitung des Unterauftragnehmers (z. B. die Nichteinhaltung von Datenschutzbestimmungen) oder bei Nichtweitergabe von Kontroll- und Überprüfungsrechten der Mandantin an die Unterauftragnehmer, hat die Mandantin das Recht von der debixx zu verlangen, dass die Verarbeitung oder Nutzung personenbezogener Daten der Mandantin nicht mehr vom Unterauftragnehmer durchgeführt wird.

h. Sollte die Mandantin selbst im Rahmen einer Auftragsverarbeitung Auftragnehmerin sein, stehen die Rechte aus dieser Vereinbarung auch deren Auftraggebern zu.

§ 7 Kontrollrechte der Mandantin

a. Die Mandantin hat das Recht, im Benehmen mit debixx Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sie hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch debixx in deren Geschäftsbetrieb zu überzeugen.

b. Soweit sich die Mandantin zur Durchführung von Kontrollen der Hilfe Dritter bedienen möchte, ist sie hierzu nur berechtigt, soweit die eingesetzten, nicht zum Unternehmen der debixx gehörenden natürlichen oder juristischen Personen einer gesetzlichen beruflichen Verschwiegenheitspflicht unterfallen.

Soweit andere Dritte mit Kontrollen befasst werden sollen, steht der debixx das Recht zu, Kontrollpersonen abzulehnen, soweit diese direkt oder indirekt Mitbewerber der debixx sind oder zur debixx in einem direkten oder indirekten Wettbewerbsverhältnis stehen; dies gilt auch, soweit die mit Kontrollen beauftragten Dritten ihrerseits als verbundene Unternehmen eines direkten oder indirekten Mitbewerbers der debixx gelten.

c. debixx stellt sicher, dass sich die Mandantin von der Einhaltung der Pflichten der debixx nach Art. 28 DS-GVO überzeugen kann. debixx verpflichtet sich, der Mandantin auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der TOMs nachzuweisen.

d. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch erfolgen durch:

1. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

2. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

3. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

4. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

e. Für die Ermöglichung von Kontrollen durch die Mandantin kann debixx eine Vergütung verlangen.

§ 8 Mitwirkungen der debixx

a. debixx unterstützt die Mandantin bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.:

1. die Sicherstellung eines angemessenen Schutzniveaus durch TOMs, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Mandantin zu melden,

3. die Verpflichtung, die Mandantin im Rahmen ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

4. die Unterstützung der Mandantin bei deren Datenschutz-Folgenabschätzung,
ee. die Unterstützung der Mandantin im Rahmen von Konsultationen mit der Aufsichtsbehörde.

5. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten der debixx zurückzuführen sind, kann debixx eine Vergütung verlangen.

§ 9 Weisungsbefugnis der Mandantin

a. Ihre mündlichen Weisungen bestätigt die Mandantin unverzüglich mindestens in Textform.

b. debixx hat die Mandantin unverzüglich zu informieren, wenn sie der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. debixx ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Mandantin bestätigt oder geändert wird.

c. Sofern nicht die Mandantin selbst, benennt diese folgende weisungsberechtigte Personen für die Verwaltung, strategische Entscheidungen und den Studiobetrieb:

Name	Position	Kontakt eMail
-	-	-
-	-	-
-	-	-
-	-	-

debixx benennt folgende Personen, die zum Empfang von Weisungen der Mandantin berechtigt sind:

Name	Position	Kontakt eMail
Frank Haße	Geschäftsleitung	Frank.hasse@debixx.com
Holger Ziegert	Geschäftsleitung	Holger.ziegert@debixx.com
-	-	-
-	-	-

Die Parteien werden einander Änderungen der Ansprechpartner schriftlich oder in Textform mitteilen. Die Änderungen werden als Anlagen Vertragsbestandteile.

d. Ist die debixx zum Ersatz eines Schadens verpflichtet, der aufgrund einer Weisung der Mandantin verursacht wurde oder sonst von dieser zu vertreten ist, stellt die Mandantin die debixx im Innenverhältnis auf erstes Anfordern frei.

e. Erteilt die Mandantin Einzelweisungen, die über die gesetzlichen Anforderungen hinausgehen, sind die dadurch begründeten Kosten von der Mandantin zu tragen.

§ 10 Löschung und Rückgabe personenbezogener Daten/Datenträgern

a. Kopien oder Duplikate der Daten werden ohne Wissen der Mandantin nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

b. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch die Mandantin - spätestens mit Beendigung der im Softwarelizenzvertrag einschließlich seiner Anlagen vereinbarten Leistungen - hat debixx sämtliche in ihren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Mandantin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

c. In Anbetracht der schnell fortschreitenden technischen Entwicklung und der sich stetig aktualisierenden Erkenntnisse wird auf die Festlegung von bestimmten Verfahren zur Löschung verzichtet. Es sind jedoch Verfahren zu nutzen, die über die Standardlöschverfahren der Betriebssysteme hinausgehen und die die personenbezogenen Daten so löschen, dass sie nicht wiederhergestellt werden können.

d. Eine Vernichtung bzw. Löschung hat, für den Fall, dass entgegenstehende gesetzliche (z. B. nach Steuer- oder Handelsrecht) oder behördliche Anordnungen bzw. Regelungen existieren, nicht zu erfolgen. Hierüber ist die Mandantin umgehend schriftlich zu informieren.

e. Sollte die Löschung von elektronischen Datenträgern nicht oder nur mit einem hohen Aufwand möglich sein, tritt an die Stelle der Löschung der Informationen die Einschränkung der Verarbeitung entsprechend der Regelungen des Art. 18 DS-GVO.

f. Die Verpflichtung zur Löschung gilt nicht für Daten, die auf Systemen gespeichert wurden, die ausschließlich dem Zwecke der Datensicherung dienen (so genannte ,,Backups"). Wiederherstellungsmaßnahmen dieser Dateien verstoßen nicht gegen die hier vereinbarten Verpflichtungen. Die redundant wiederhergestellten Daten sind jedoch umgehend zu vernichten bzw. zu löschen.

g. Dokumentationen bzw. Informationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, bzw. einem ordnungsgemäßen Umgang mit den Daten dienen, sind durch debixx entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. debixx kann sie der Mandantin bei Vertragsende zu ihrer Entlastung übergeben.

h. Die Parteien vereinbaren, dass zeitgleich mit Inkrafttreten dieser Vereinbarung die zwischen den Parteien bestehende Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 BDSG a.F. sowie etwaige weitere Vereinbarungen zur Auftragsdatenverarbeitung einvernehmlich beendet und durch diese neue Vereinbarung zur Auftragsverarbeitung ersetzt werden.

Anlage 4 „Technisch-Organisatorische Maßnahmen (TOMs)“

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sind geeignete TOMs zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Nachfolgend sind die TOMs der debixx konkret beschrieben. Da diese Maßnahmen dem technischen Fortschritt und der steten Weiterentwicklung unterliegen, behält sich debixx vor, statt der beschriebenen Maßnahmen adäquate alternative Maßnahmen einzusetzen. Das Schutzniveau der festgelegten Maßnahmen wird bei solchen Änderungen nicht unterschritten werden.

1. Pseudonymisierung und Verschlüsselung
(Art. 32 Abs. 1 lit. a DS-GVO, Art. 25 Abs. 1 DS-GVO)
Regelungsgegenstand sind Maßnahmen, um physische, materielle oder immaterielle Schäden bzw. Beeinträchtigungen der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den im Auftrag verarbeiteten Daten zu vermeiden.

- Eine Verschlüsselung für den Transport von Daten auf Dateiebene findet statt;
- Beim physischen Transport und Versand von Daten erfolgt eine komplette Verschlüsselung des Datenträgers auf Basis AES 256-Bit. Alternativ kann nach vorheriger kostenpflichtiger Beauftragung eine softwareseitige Verschlüsselung einer bestehenden USB-Festplatte aufgesetzt werden;
- Soweit mobile Datenträger zum Einsatz kommen, werden darauf befindliche Inhalte verschlüsselt. Hierfür stehen hardwarebasierte und softwarebasierte Verfahren zur Verfügung. Alle Datenträger in Notebooks sind mit einer Disk-Encryption verschlüsselt, welche alle Partitionen umfasst;
- Alle geschäftlich eingesetzten Smartphones der Mitarbeiter der debixx sind in einem Mobile Device Management, welches die Daten in einem verschlüsselten Container speichert und im Falle eines Verlusts ein Fernlöschen ermöglicht.

2. Vertraulichkeit
(Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Regelungsgegenstand sind Maßnahmen zur Verwehrung des Zutritts zu Datenverarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (physikalische Sicherheit).

- Die Server der debixx werden in einer Liegenschaft mit verschlossenem Serverraum betrieben. Die Liegenschaft ist als geschlossener Sicherheitsbereich konzipiert, mit einer Aufteilung in unterschiedliche Sicherheitszonen (Besucherbereich, Büroräume, Facility Management, Technikräume und Serverraum). Es besteht sowohl baulicher als auch technischer Zutrittsschutz. Der Serverraum ist durch eine Schließanlage gesichert. Zutritt haben nur autorisierte Mitarbeiter;

- Die Mitarbeiter der debixx unterliegen einem Rollenkonzept. Dieses regelt die Identifikation der Mitarbeiter durch Chip, zu welchen Bereichen der Mitarbeiter Zutritt hat und wer welche Schlüssel hat;

- Besucher, einschließlich Dienstleister, müssen sich anmelden und haben nur beaufsichtigten Zutritt. Der Besuch wird protokolliert. Besucher werden schriftlich angemeldet, auf das Datengeheimnis verpflichtet, am Empfang abgeholt und durch Mitarbeiter in den Unternehmensräumen, sowie nach dem Besuch bis zum Ausgang begleitet;

- In allen Räumlichkeiten gilt zudem eine Ausweispflicht für Besucher. Besucherausweise werden am Eingang ausgegeben. Alle Mitarbeiter sind darauf geschult, Personen, die allein und ohne Ausweis in den Räumlichkeiten angetroffen werden, anzusprechen und zum Empfang zu begleiten;

Zugangskontrolle
Regelungsgegenstand sind Maßnahmen zur Verwehrung des Zugangs zu Datenverarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (logische Sicherheit).

- Erfolgen administrative Tätigkeiten über externe Zugänge, sind diese sogenannten VPN-Verbindungen immer gemäß aktueller Technik verschlüsselt und es ist eine zusätzliche Authentifizierung erforderlich;
- Die Identifikation mit Benutzernamen und sicherem Passwort ist obligatorisch. Benutzer werden automatisch nach drei Fehlversuchen zur Anmeldung gesperrt. Eine Reaktivierung des Benutzeraccounts erfolgt automatisch nach einer gewissen Zeitspanne. Kenn-/ Passwörter müssen alle 90 Tage gewechselt werden. Eine Automatik verhindert, dass als neues das alte Passwort gewählt wird**.** Die Aufzeichnung oder Speicherung von Passwörtern im Klartext ist gemäß Benutzerrichtlinie verboten;
- Die Grundlage zur Vergabe der Berechtigungen in allen Systemen bildet die Rollen- und Rechtematrix, welche die Berechtigungen an die Zuständigkeit der jeweiligen Fachabteilung bindet. Hierdurch wird die Anzahl der Administratoren auf das Notwendigste reduziert. Die Benutzeraccounts sind grundsätzlich personalisiert, ausgenommen Benutzeraccounts für Services. Benutzer-Accounts werden im Rahmen der Dokumentation beim Tätigkeitsbeginn neuer Mitarbeiter vergeben;
- Anmeldungen auf der Betriebssystemebene werden über Eventlogs protokolliert;
- Es gibt einen Virenschutz auf den Servern und den lokalen Systemen;
- Im Rahmen der Auftragsverarbeitung werden nur Mitarbeiter eingesetzt, die die mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht wurden und die für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses zur Verschwiegenheit verpflichtet sind;

Zugriffskontrolle
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf Daten zugreifen können, für die sie zugriffsberechtigt sind und dass personenbezogene Daten bei der Verarbeitung, Nutzung oder nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Alle EDV-Zugriffe sind mit Benutzerprofil und Kennwort gesichert;
- CD-Laufwerke und USB-Schnittstellen sind für Benutzer gesperrt;
- Es gibt einen Zugriffsschutz durch Bildschirmschoner mit automatischer Sperrung und ausschließlich passwortgeschützter Aufhebung;
- Alle Benutzer müssen bei Verlassen des Arbeitsplatzes ihren Rechner sperren, die Vorgaben dazu sind in der Benutzerrichtlinie geregelt. Zudem sperrt sich der Rechner nach einigen Minuten der Inaktivität selbst;
- Passwörter werden nach einer internen Passwort-Richtlinie vergeben, welche die Komplexität vorgibt und auch in Form von Gruppenrichtlinien im Active-Directory umgesetzt ist, um den Einsatz sicherer Passwörter zu erzwingen. Die Passwörter haben nur eine begrenzte Gültigkeit und werden innerhalb eines definierten Zeitraums geändert;
- Zugriffsrechte werden auf Basis betrieblicher Erfordernisse vergeben;
- Sämtliche administrativen Zugriffe werden protokolliert;
- Die Zugriffsrechte werden ständig aktualisiert, sowie anlassbezogen angepasst, z.B. beim Abteilungswechsel eines Mitarbeiters innerhalb des Unternehmens oder beim Ausscheiden aus dem Unternehmen;
- Es gibt ein Fernwartungskonzept;

Trennungskontrolle
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

- Die Trennung erfolgt überwiegend auf Basis der Anwendung, die für die Mandantin betrieben wird. Debixx trennt alle Daten mindestens logisch auf Ebene einer Mandantin;
- Soweit eine gemeinsame Nutzung eines Systems mit mehreren Mandaten erfolgt, findet eine logische Trennung der Mandanten statt. Mandanten haben keinen Zugriff auf die Inhalte und Daten eines anderen Mandanten bei debixx.

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

Weitergabekontrolle
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Personenbezogene Daten, die Gegenstand der Auftragsverarbeitung sind, werden ausschließlich in den Rechenanlagen der debixx und autorisierter Auftragsverarbeiter verarbeitet. Eine Speicherung auf Datenträgern außerhalb der Rechenanlagen findet nur im Rahmen eines Datentransportes statt. Der Transport von Datenträgern erfolgt ausschließlich verschlüsselt. Datenträger, die nicht weiterverwendet werden sollen, werden vernichtet. Die Vernichtung erfolgt bei debixx vor Ort im Beisein eines Mitarbeiters von debixx und wird protokolliert;
- Für die Datenträger innerhalb der geschützten Rechenzentren hat debixx interne Standards für den Umgang mit Berechtigungen im Rahmen eines Berechtigungs- und Rollenkonzepts definiert. Dieses regelt u. a. die Berechtigung von Administratoren auf den für die Mandantin betriebenen Systemen. Darin werden beispielsweise Anforderungen an sichere Kennworte definiert;
- Die IT-Systeme der debixx sind durch Firewall-Technologien gegen Eingriffe von außen abgeschirmt. Ergänzend gelten die Zugangskontrollmaßnahmen;
- Alle lokalen Datenträger in mobilen Endgeräten sind mittels Laufwerkverschlüsselung vollverschlüsselt;
- Mobile Datenträger dürfen bei debixx nur im Support ausschließlich an dafür vorgesehene Geräte angeschlossen und genutzt werden;
- Die Verwendung nicht geschäftlich beschaffter/genutzter Datenträger ist untersagt;
- Das Speichern von personenbezogenen Daten auf Wechseldatenträgern in unverschlüsselter Form ist den Mitarbeitern der debixx durch interne Richtlinien untersagt;
- Im Bedarfsfall werden die Daten dem jeweiligen Kunden auf unserem SFTP Server bereitgestellt;
- Die Übertragung von personenbezogenen Daten erfolgt ausschließlich über verschlüsselte VPN-Technik oder dedizierte MPLS-Netze (nicht öffentliche Netze). Die Gegenstelle wird hierbei fest angelegt und protokolliert;
- Der Zugriff auf Server der debixx bzw. ihre Provider erfolgt mittels SSL/TLS-Verschlüsselung;
- Für die betriebsnotwendigen Kopien, z. B. im Rahmen von Datensicherungen, werden nur dokumentierte Verfahren genutzt;
- Soweit im Rahmen der vertraglichen Leistungen ein physischer Transport von personenbezogenen Daten auf Datenträgern erforderlich ist, erfolgt dieser Transport ausschließlich auf verschlüsselten Medien;
- Soweit Datenträger versendet werden müssen, erfolgt der Versand entweder verschlüsselt, oder in speziellen verschlossenen Transportboxen, durch einen speziellen Dienstleister. Alternativ hat der Auftraggeber auch die Möglichkeit einen Transport selbst zu beauftragen oder zu organisieren. Der Empfänger wird im Ticketsystem dokumentiert;
- Eine Weitergabe von Daten an Dritte erfolgt nur soweit zwischen den Parteien zur Leistungserbringung vereinbart oder auf schriftliche Weisung der Mandantin;
- Übermittlungswege und Datenempfänger werden festgelegt und dokumentiert;
- Die jeweiligen Verpflichtungen sind Gegenstand der Benutzerrichtlinie. Die Mandantin hat die Möglichkeit, eine kostenpflichtige E-Mail-Verschlüsselung zu beauftragen;

Eingabekontrolle
Regelungsgegenstand sind Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Eingaben an Systemen können nur durch Mitarbeiter erfolgen, die aufgrund ihres Aufgabenbereichs Zugriff haben. Der Umfang der Berechtigungen wird durch eine Rollen- und Rechtematrix gewährleistet;
- Konfigurationseingaben erfolgen ausschließlich über dafür vorgegebene Zugriffe und Werkzeuge;

Vermeidung von Beschädigungen
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

- Sämtliche Speichersysteme sind redundant ausgelegt (gespiegelte Festplatten). Alle Kundensysteme und deren Inhalte werden regelmäßig gesichert, sofern dies von der Mandantin beauftragt wurde. Darüber hinaus kann die Mandantin weitere Redundanzen kostenpflichtig beauftragen. Bei einer Fehlfunktion des Systems befinden sich alle personenbezogenen Kundendaten unbeschädigt in einer entsprechenden Sicherung;

Auftragskontrolle
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Mandantin verarbeitet werden können.

- Eine Datenverarbeitung im Auftrag erfolgt grundsätzlich nur auf der Grundlage eines schriftlichen Vertrages, wobei auch der Abschluss in elektronischer Form möglich ist. Die Datenverarbeitung findet dabei nur zum Zwecke der jeweiligen Vertragserfüllung statt. Ist ein Vertrag geschlossen, so wird für jede Mandantin ein Benutzerprofil in einem Datenblatt festgelegt. Dort sind auch der Umfang des Auftrages und die jeweiligen Ansprechpartner hinterlegt. Durch

interne Anweisungen ist die Voraussetzung geschaffen, dass der Service Desk und das Service Management der debixx die Daten nur im Rahmen der Beauftragung und ordnungsgemäß erteilter Weisungen verarbeitet;

- Sofern debixx im Rahmen einer Auftragsverarbeitung Unteraufträge erteilt, erfolgt die Auswahl des Unterauftragnehmers unter Beachtung der gesetzlich geforderten Sorgfaltspflichten, insbesondere hinsichtlich der Datensicherheit;
- Vor und nach Vertragsschluss wird die Dokumentation der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen nach Maßgabe der gesetzlichen Vorgaben regelmäßig geprüft.

3. Verfügbarkeit und Belastbarkeit
(Art. 32 Abs. 1 lit. b DS-GVO)
Verfügbarkeitskontrolle
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und die das Risiko, dass nicht alle Funktionen des Systems aufgrund von Systemüberlastungen zur Verfügung stehen, reduzieren und dass Fehlfunktionen gemeldet werden.

- Der Schutz vor Datenverlust durch technisches Versagen oder z. B. versehentliches Löschen durch den Anwender und die Möglichkeiten der Wiederherstellung in diesen Fällen werden durch die Datensicherungsverfahren gemäß der jeweiligen Leistungsbeschreibung geregelt. Alle Systeme werden regelmäßig mit Datensicherungsmaßnahmen gesichert. debixx realisiert auch unterschiedliche optionale Verfahren, die entsprechend dem Schutzbedarf der Daten beauftragt werden können. Wesentliche Parameter sind die Verfügbarkeit und die Wiederherstellungszeit im Fehlerfall. Tägliche Sicherungen mit den Backup-Systemen sind rückwirkend für die letzten drei Monate wiederherstellbar;
- Die Wiederherstellungen werden getestet;
- Die Datensicherungen werden in einem feuerfesten Tresor gelagert, um einen physischen Verlust zu vermeiden;
- Es werden technische Maßnahmen nach internen Standards ergriffen, um einen Befall der Datenverarbeitungsanlagen der debixx mit Schadsoftware zu vermeiden (Virenschutz);
- Es gibt eine unterbrechungsfreie Stromversorgung (USV);
- Die Plattenspeicher sind fest montiert;

Rasche Wiederherstellbarkeit
(Art. 32 Abs. 1 lit. c DS-GVO)
Regelungsgegenstand sind Maßnahmen, die gewährleisten, dass die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- Die Datenwiederherstellung im Falle eines Systemausfalls erfolgt nach dem RestoreKonzept. Art und Dauer des Wiederherstellverfahrens ist dabei abhängig vom Datenvolumen, der eingesetzten Backup-Methode, den Backupmedien und der Infrastruktur.

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle: debixx wird keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung der Mandantin machen, etwa mittels eindeutiger Vertragsgestaltung, formalisiertem Auftragsmanagement, strenger Auswahl des Dienstleisters, einer Vorabüberzeugungspflicht und Nachkontrollen.

5. Organisatorische Maßnahmen

- Bestellung eines betrieblichen Datenschutzbeauftragten;
- Verpflichtung aller Mitarbeiter auf die Vertraulichkeit der Daten (Art. 5 i.V.m. Art. 24, 29, 32 DS-GVO);
- Datenschutzunterweisungen und innerbetriebliche Schulungen der Mitarbeiter;
- Aktenschränke einzeln abschließbar;
- Feuerlöscher und Brandmelder;
- Datenschutzgerechte Aktenvernichtung