Vereinbarung zur Auftragsverarbeitung für „Flexopus“
Version 3.0, Stand: 01.01.2025

§ 1 Vertragspartner, Geltungsbereich

1. Diese Vereinbarung gilt nur für Kunden, die Unternehmer (§ 14 BGB), eine juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen sind ("Kunde").
2. Diese Vereinbarung gilt für sämtliche Verarbeitungen von personenbezogenen Daten durch Flexopus GmbH, Schlosserstraße 2, 70180 Stuttgart, HRB 781714 (nachfolgend "Flexopus") im Auftrag des Kunden.

§ 2 Geltungsdauer der Vereinbarung

1. Die Geltungsdauer dieser Vereinbarung entspricht der des Hauptvertrags.

§ 3 Gegenstand, Art und Zweck der Verarbeitung

1. Gegenstand, Art und Zweck der Verarbeitung ergeben sich aus den Allgemeinen Geschäftsbedingungen in Zusammenhang mit der jeweiligen Leistungsbeschreibung (nachfolgend zusammen „Hauptvertrag“).

§ 4 Art der personenbezogenen Daten und Kategorien der Betroffenen

1. Es werden, je nach konkreter Nutzung, folgende Arten von personenbezogenen Daten verarbeitet:
    a. Stammdaten (z.B. Name),
    b. Kontodaten (z. B. Nutzername, Passwort),
    c. Profildaten (z. B. Profilfoto, Sprache, Favoriten),
    d. Kontaktdaten (z. B. E-Mail, Telefonnummer, Adresse),
    e. Inhaltsdaten (z. B. Texteingaben),
    f. Nutzungsdaten (z. B. besuchte Webseiten, Zugriffszeiten),
    g. Zahlungsdaten (z. B. Rechnungen, Zahlungsmethode),
    h. Vertragsdaten (z. B. abgeschlossene Abonnements),
    i. Geräte- und serverseitige Daten (z. B. Geräteinformationen, IP-Adressen),
    j. Daten zur Buchung über die Softwarelösung durch Betroffenen (z. B. Art der Buchung, Zeitraum der Buchung, Kalendereintrag, eingeladene Personen inkl. Kontaktdaten, Check-in/Check-out, Zusatzmerkmale, Nutzer- und Anwendungs-Logs)
2. Von der Verarbeitung betroffen sind folgende Personenkreise:
    a. Mitarbeiter / Beschäftigte des Kunden
    b. Endkunden / Besucher / Ansprechpartner des Kunden
    c. Interessenten des Kunden

§ 5 Ort der Datenverarbeitung

1. Die Verarbeitung der personenbezogenen Daten findet ausschließlich in einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

§ 6 Ansprechpartner / Datenschutzbeauftragter

1. Flexopus hat einen Datenschutzbeauftragten bestellt, der dem Kunde für datenschutzrechtliche Auskünfte als Ansprechpartner zur Verfügung steht:
   PROLIANCE GmbH
   Leopoldstr. 21
   80802 München
   datenschutzbeauftragter@datenschutzexperte.de
   Bitte nennen Sie bei der Kontaktaufnahme mit dem Datenschutzbeauftragten die Flexopus GmbH direkt im Betreff.
2. Für Weisungen des Kunden stehen zudem folgende Ansprechpartner zur Verfügung:
    a. Philipp Wahju, Geschäftsführer
       E-Mail: mail@flexopus.com,
       Telefon +49 711 342 085 05
    b. Markus Merkle, Datenschutzkoordinator
       E-Mail: privacy@flexopus.com,
       Telefon +49 711 342 085 05
3. Weisungsberechtigte Personen des Verantwortlichen teilt der Kunde Flexopus unverzüglich nach Vertragsschluss in Textform mit und übermittelt dabei insbesondere Vorname, Nachname, Organisationseinheit, E-Mail-Adresse und Telefon.
4. Soweit vom Kunde keine weisungsberechtigte Person benannt wird, wird davon ausgegangen, dass der für die Nutzung der Flexopus Plattform beim Kunden hinterlegte Systemadministrator weisungsberechtigt im Sinne dieser Vereinbarung ist.
5. Die weisungsberechtigte Person ist überdies berechtigt und bevollmächtigt, Erklärungen zu etwaigen Ergänzungen und/oder Änderungen dieser Vereinbarung entgegenzunehmen und anzunehmen.
6. Änderungen diesbezüglich teilen sich die Vertragsparteien unverzüglich mit.

§ 7 Weisungsgebundenheit

1. Flexopus darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden verarbeiten. Flexopus verwendet darüber hinaus die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind sowie personenbezogenen Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. Eine Ausnahme von der Weisungsgebundenheit gilt nur, sofern Flexopus gesetzlich zur Verarbeitung verpflichtet ist. Sofern solche Verpflichtungen für Flexopus bestehen, teilt Flexopus diese dem Kunde vor der Verarbeitung mit, es sei denn, das

betreffende Recht verbietet eine solche Mitteilung wegen eines wichtigen öffentlichen Interesses.

3. Soweit eine betroffene Person sich mit einer Berichtigungs-, Löschungs- oder sonstiger Aufforderung in Bezug auf ihn betreffende personenbezogene Daten unmittelbar an Flexopus wendet, wird Flexopus dieses Ersuchen unverzüglich an den Kunde weiterleiten.
4. Flexopus informiert den Kunde unverzüglich, falls Flexopus der Auffassung ist, dass eine Weisung gegen die Datenschutzgrundverordnung (DSGVO) oder gegen sonstige Datenschutzbestimmungen verstößt. Flexopus ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis die weisungsberechtigte Person des Kunden die Weisung so angepasst hat, dass sie im Einklang mit der Datenschutzgrundverordnung (DSGVO) und den sonstigen Datenschutzbestimmungen steht.
5. Mündliche Weisungen bestätigt der Kunde unverzüglich mindestens in Textform.

§ 8 Technische und organisatorische Maßnahmen

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft Flexopus geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2. Die mindestens zu ergreifenden technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit sind in dem Datensicherheitskonzept in Anlage 1 niedergelegt.
3. Flexopus kann die technischen und organisatorischen Maßnahmen anpassen, sofern und soweit dabei das in Anlage 1 niedergelegte Sicherheitsniveau nicht unterschritten wird.
4. Flexopus führt zur Gewährleistung eines angemessenen Datenschutzniveaus notwendige personelle Maßnahmen durch. Diese sind insbesondere: sorgfältige Auswahl des Personals, Eingangs- sowie jährliche Folgeschulungen.

§ 9 Verpflichtung zu Vertraulichkeit und Verschwiegenheit; Informationspflichten über behördliche Maßnahmen

1. Flexopus setzt bei der Verarbeitung nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet wurden bzw. einer gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Flexopus wird den Kunden über Kontrollhandlungen und – maßnahmen von Aufsichts- und Ermittlungsbehörden, soweit sich diese auf die Verarbeitung im Auftrag beziehen, unverzüglich informieren, es sei denn eine solche Mitteilung ist aufgrund von Unions- oder deutschem Recht unzulässig.

§ 10 Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, insbesondere keine Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice. Flexopus ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Die Unterbeauftragung von weiteren Auftragsverarbeitern ist zulässig. Voraussetzung ist, dass
    a. Flexopus Namen und Anschrift des geplanten Unterauftragnehmers eine angemessene Zeit vor der Beauftragung in Textform mitteilt,
    b. Flexopus vertraglich sicherstellt, dass die vereinbarten Regelungen zwischen Kunde und Flexopus auch gegenüber dem Unterauftragnehmer gelten, und
    c. der Kunde der geplanten Unterbeauftragung nicht innerhalb von 2 Wochen nach Mitteilung über den geplanten Einsatz widerspricht.
3. Der Kunde ist berechtigt, von Flexopus Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.
4. Die derzeit genehmigten Unterauftragnehmer ergeben sich aus Anlage 2.
5. Die Weitergabe von personenbezogenen Daten des Kunden an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet, insbesondere muss der Unterauftragnehmer die Verpflichtungen nach Art. 28 DS-GVO und die Einhaltung der hier getroffenen Regelung dieser Vereinbarung sicherstellen.
6. Widerspricht der Kunde dem geplanten Einsatz des Unterauftragnehmers, gilt Ziffer 6.2. der Allgemeinen Geschäftsbedingungen, Allgemeiner Teil entsprechend.

§ 11 Pflicht zur Unterstützung des Kunden hinsichtlich der Rechte Betroffener

1. Flexopus hat den Kunden bei der Wahrung der in Kapitel III der DSGVO genannten Rechte der Betroffenen, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Sperrung und Löschung zu unterstützen. Flexopus hat eine Berichtigung, Löschung oder Sperrung von personenbezogenen Daten, die der Betroffene von dem Kunde rechtmäßig verlangt, im Benehmen mit dem Kunde unverzüglich vorzunehmen.
2. Flexopus verpflichtet die beauftragten Unterauftragnehmern vertraglich entsprechend im Hinblick auf die Benachrichtigung,

Auskunftserteilung, Berichtigung, Sperrung und Löschung.

3. Flexopus hat dem Kunde alle Auskünfte zu erteilen, die zur Erfüllung von Auskunftspflichten des Kunden gegenüber dem Betroffenen erforderlich sind, sofern und soweit die entsprechenden Informationen Flexopus vorliegen und/oder auf Weisung des Kunden dem Betroffenen selbst Auskunft zu erteilen.
4. Flexopus ist berechtigt, dem Kunde Aufwände für die Erbringung von Unterstützungsleistungen gemäß diesem § 11 in Höhe der üblichen Sätze von Flexopus in Rechnung zu stellen.

§ 12 Unterstützung bei der Erfüllung der Pflichten aus Art. 32 bis 36 DS-GVO

1. Flexopus wird unter Berücksichtigung der Art der Verarbeitung und der zur Verfügung stehenden Informationen den Kunde bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützten. Hieraus ergeben sich für Flexopus unter anderem nachfolgende Pflichten.
2. Flexopus teilt dem Kunde Verletzungen des Schutzes im Zusammenhang mit den im Auftrag des Kunden verarbeiteten personenbezogenen Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis von Flexopus vom relevanten Ereignis an die weisungsberechtigte Person des Kunden zu erfolgen. Sie muss, sofern und soweit Flexopus vorliegend, mindestens folgende Angaben enthalten:
    a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
    b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
    c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    d. eine Beschreibung der von Flexopus ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
3. Flexopus verpflichtet sich, den Kunde im Rahmen seiner Informationspflichten nach Artikel 34 DSGVO gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen, sofern und soweit diese Flexopus vorliegen, unverzüglich zur Verfügung zu stellen.
4. Sofern und soweit nicht alle in § 12 genannten Informationen zur gleichen Zeit bereitgestellt werden können, wird Flexopus weitere Informationen nachliefern, sofern und sobald sie verfügbar sind.
5. Flexopus wird laufend überprüfen, ob eine Form der Verarbeitung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO bedarf.
6. Flexopus ist verpflichtet, den Kunden bei Konsultation der Aufsichtsbehörden nach Art. 36 DS-GVO zu unterstützen. Seine eigenen Pflichten aus Art. 36 DS-GVO bleiben hiervon unberührt.
7. Flexopus ist berechtigt, dem Kunde Aufwände für die Erbringung von Unterstützungsleistungen gemäß diesem § 12 in Höhe der üblichen Sätze von Flexopus in Rechnung zu stellen.

§ 13 Allgemeine Unterstützungspflichten

1. Die Parteien arbeiten hinsichtlich Anfragen von Aufsichtsbehörden zusammen. Soweit der Kunde einer Kontrolle durch Aufsichts- und/oder Ermittlungsbehörden ausgesetzt ist, wird Flexopus nach besten Kräften unterstützen.

§ 14 Löschung und Rückgabe von personenbezogenen Daten

1. Nach Beendigung der Vereinbarung löscht Flexopus sämtliche im Auftrag verarbeitete personenbezogene Daten oder gibt diese an den Kunde zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.
2. Flexopus verpflichtet die beauftragten Unterauftragnehmern vertraglich entsprechend zur Löschung und Rückgabe.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch Flexopus über das Vertragsende hinaus aufzubewahren. Flexopus kann sie zu seiner Entlastung bei Vertragsende dem Kunde übergeben.

§ 15 Kontrollrechte des Kunden

1. Flexopus stellt dem Kunden alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in dieser Vereinbarung festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Kunden gestattet Flexopus ebenfalls die Prüfung der unter diese Vereinbarung fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Kunde einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) sowie eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
2. Soweit nicht aus von dem Kunde zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener

Vorankündigung und zu Geschäftszeiten von Flexopus statt.

3. Den mit der Kontrolle betrauten Personen ist von Flexopus soweit erforderlich Zutritt und Einblick zu ermöglichen.

§ 16 Beendigung der Vereinbarung

1. Flexopus ist berechtigt, diese Vereinbarung ohne Einhaltung einer Frist zu kündigen, wenn der Kunde auf die Erfüllung einer Weisung besteht, nachdem der Kunde von Flexopus darüber in Kenntnis gesetzt wurde, dass die erteilte Weisung gegen geltende datenschutzrechtliche Bestimmungen verstößt und der Kunde die entsprechende Weisung nicht so anpasst, dass sie im Einklang mit den geltenden datenschutzrechtlichen Bestimmungen steht (vgl. § 7 (4)).
2. Unbeschadet dessen kann diese Vereinbarung nur zusammen mit der betroffenen Vertragsleistung gekündigt werden. Nach Beendigung der Vereinbarung hat der Kunde die Nutzung der entsprechenden Vertragsleistung unverzüglich einzustellen und ist insbesondere nicht berechtigt die Flexopus Plattform weiter zu nutzen.
3. Ziffer 16 der Allgemeinen Geschäftsbedingungen, Allgemeiner Teil gilt entsprechend.

§ 17 Haftung

1. Es gilt die gesetzliche Haftung nach Art. 82 DS-GVO.
2. Unbeschadet dessen ist die Haftung von Flexopus im Innenverhältnis ausgeschlossen, sofern und soweit Flexopus gemäß dieser Vereinbarung und gemäß den Weisungen des Kunden handelt. Der Kunden stellt Flexopus insofern von sämtlichen Schadensersatzansprüchen betroffener Personen frei, sofern und soweit diese nicht darauf beruhen, dass Flexopus gegen ihm als Auftragsverarbeiter obliegende Pflichten verstoßen hat oder im Auftrag verarbeitete personenbezogene Daten ohne oder gegen eine Weisung des Kunden verarbeitet hat.

§ 18 Sonstiges

1. Ziffer 17 der Allgemeinen Geschäftsbedingungen, Allgemeiner Teil gilt entsprechend.

Flexopus

Anlage 1 – Technische und organisatorische Maßnahmen (TOM) für „Flexopus“
Letzte Aktualisierung: 01.01.2025

I. Maßnahmen zur Vertraulichkeit

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Absicherung von Gebäudeschächten/Dachfenstern o.ä. - Gebäudeschächte etc. sind ordnungsgemäß abgesichert
- Besucherprotokollierung - Sicherheitskontrollen und Besucherbuch, Begleitung des Besuchs im Büro
- Empfang - Besucherkontrolle am Empfang
- Festgelegte Reinigungszeiten - Reinigungszeiten sind vorab definiert
- Reinigungspersonal - Das Reinigungspersonal wurde sorgfältig ausgewählt
- Schließsystem - elektronisch - Türsicherungen (elektrische Türöffner) in Verbindung mit dem Zutrittskontrollsystem
- Schließsystem - mechanisch - Verschlossene Türen bei Abwesenheit
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel
- Videoüberwachung außerhalb der Geschäftszeiten

2. Beschreibung der Zugangskontrolle

Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Authentifizierung mit Benutzername und Passwort - Persönlicher und individueller User Log-In bei Systemanmeldung und bestimmten Anwendungen
- Authentifizierung bei Fernzugängen - Persönlicher und individueller User Log-In bei Anmeldung im System bzw. Unternehmensnetzwerk
- Automatische Bildschirmsperre - Sperrung von Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatisierte Pausenschaltung)
- Firewall - Hardwarefirewall und Softwarefirewall
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Gesichertes WLAN

3. Beschreibung der Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Berechtigungskonzept
  - Einsatz eines Berechtigungskonzepts
  - Verwaltung von Berechtigungen
  - Differenzierte Berechtigungen
  - Profile- und Rollenkonzept
  - Dokumentation von Berechtigungen
  - Anzahl Administratoren-Rollen so gering wie möglich
  - Differenzierung administrativer Aufgaben
  - Autorisierungsprozess für Berechtigungen
  - Genehmigungsroutinen
- Entsorgung von Datenträgern - Datenträgervernichtung (DIN 66399) Protokollierung der Vernichtung (z.B. Vernichtungs-Zertifikat durch Dienstleister); physische Löschung von Datenträgern vor Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Entsorgung Papierunterlagen - Einsatz von Aktenschreddern und / oder Protokollierung der Vernichtung (z.B. Vernichtungs-Zertifikat durch Dienstleister)
- Passwortlichtlinien - Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- Zwei-Faktor Authentifizierung (sofern technisch möglich)
- Sichere Aufbewahrung Unterlagen und Datenträgern

4. Beschreibung der Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern 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. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- SSL / TLS Verschlüsselung - Einsatz von TLS-Verschlüsselung bei der Datenübertragung im Internet
- Getunnelt Datenfernverbindungen (VPN=Virtual Private Network)
- Weitergabe in anonymisierter oder pseudonymisierter Version
- Datenträgervernichtung nach DIN 66399
- Klare Zuständigkeiten für Löschung

5. Beschreibung des Trennungsgebots:

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene personenbezogenen Daten getrennt verarbeitet werden können. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten

- Datensätze werden mit Zweckattributen / Datenfeldern versehen
- Verwendung von Testdaten

6. Beschreibung der Pseudonymisierung

Es werden folgende Maßnahmen getroffen:

- Trennung von Kontaktdaten und anderen personenbezogenen Daten
- Trennung von Kundenstammdaten und Auftragsdaten
- Frühzeitige Pseudonymisierung personenbezogener Daten (Frist für die Pseudonymisierung kann vom Kunde individuell definiert werden)
- Pseudonymisierung bei Analysedatenbanken

7. Beschreibung der Verschlüsselung

Es werden folgende Maßnahmen getroffen:

- Verschlüsselte Datenübertragung nach dem Stand der Technik: Die personenbezogenen Daten werden bei der Übertragung mit dem üblichen TLS verschlüsselt. Passwörter werden salted und gehasht gespeichert. Sessions werden verschlüsselt gespeichert, wobei eine symmetrische Verschlüsselung mit einem Anwendungsschlüssel verwendet wird.

II. Maßnahmen zur Integrität

1. Beschreibung der Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Systemseitige Protokollierung / Logfileprotokolle (Dauer der Speicherung kann vom Kunde individuell definiert werden)
- Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe

III. Maßnahmen zur Verfügbarkeit und Belastbarkeit

1. Beschreibung der Verfügbarkeitskontrolle

Durch die Verfügbarkeitskontrolle wird gewährleistet, dass personenbezogene Daten gegen den zufälligen Verlust geschützt sind. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Antivirensoftware - Einsatz von Virenschutz/Firewall
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
    - Die personenbezogenen Daten von Flexopus werden in einem Serverraum eines Drittdienstleisters gespeichert. Die Flexopus GmbH selbst betreibt keinen Serverraum und keine physische Datenspeicherung in ihren Räumlichkeiten
- Rauchmelder vorhanden
- Redundante Datenhaltung - Spiegeln von Festplatten und Back-up Verfahren
- Serverraum (Maßnahmen beziehen sich rein auf Serverzentrum des Hosting-Subdienstleisters laut Anlage 2)
    - Brandschutz - Feuerlöschgeräte im Serverraum vorhanden
    - Klimaanlage - Klimaanlage in Serverräumen vorhanden
    - Temperaturüberwachung - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen vorhanden
    - Stromversorgung - USV vorhanden
    - Videoüberwachung im Serverraum
    - Lastausgleich (Load-Balancing)
    - Automatisches Benachrichtigungssystem bei Erreichen der maximalen Auslastung
    - Alarmmeldung bei unberechtigten Zutritten in den Serverraum
    - Automatisches Benachrichtigungssystem bei Ausfall
    - Schutzsteckdosenleisten im Serverraum

2. Beschreibung der raschen Wiederherstellbarkeit

Durch die Verfügbarkeitskontrolle wird gewährleistet, dass personenbezogene Daten gegen den zufälligen Verlust geschützt sind. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Datenwiederherstellungen - Testen der Datenwiederherstellung
- IT-Notfallpläne und Wiederanlaufpläne vorhanden

IV. Weitere Maßnahmen zum Datenschutz

1. Beschreibung der Auftragskontrolle

Die Maßnahmen dienen der Sicherstellung, dass personenbezogene Daten nur auf Weisung des Verantwortlichen unter Einhaltung der datenschutzrechtlichen Bestimmungen verarbeitet werden. Um dies sicherzustellen, werden folgende Maßnahmen getroffen:

- Audits - Regelmäßige Datenschutzaudits des externen Datenschutzbeauftragten
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO
- DSB - Benennung eines Datenschutzbeauftragten
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter, regelmäßig stattfindende Nachschulungen
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO

2. Beschreibung des Managementsystems zum Datenschutz

Es werden folgende Maßnahmen zur Sicherstellung der Einhaltung der datenschutzrechtlichen Vorgaben getroffen:

- Audits - Durchführung regelmäßiger interner Audits
- Datenschutzfreundliche Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. Art. 25 Abs. 2 DSGVO

- Managementsystem für Datenschutz - Bestehendes Managementsystem zum Datenschutz (DSMS) vorhanden
- Managementsystem Informationssicherheit - Managementsystem zur Informationssicherheit (ISMS) vorhanden
- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z. B. Penetrationstest)
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Schulung/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter
- Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
- Richtlinien zur Gewährleistung von technisch-organisatorischer Maßnahmen zur Sicherheit der Verarbeitung

Flexopus

Anlage 2 – von Flexopus zur Erbringung der Dienstleistung eingesetzte Subunternehmer
Letzte Aktualisierung: 01.01.2025

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

Nr.	Name des Unternehmens	Anschrift des Unternehmens	Region, in der die Verarbeitung erfolgt	Erbrachte Leistungen
1	Hetzner Online GmbH	Industriestraße 25 91710 Gunzenhausen Deutschland	EU	Serveranbieter für Hosting, Bereitstellung IaaS
2	RapidMail GmbH	Wentzingerstr. 21 79106 Freiburg im Breisgau Deutschland	EU	SMTP-Anbieter: Versand aller Arten von E-Mails der Flexopus Plattform; ausgenommen TKG-Dienstleistungen, insbesondere Senden, Übertragen und Empfangen des Kommunikationsinhalts.
3	Mailjet SAS	13-13 bis, rue de l'Aubrac 75012 Paris Frankreich	EU	SMTP-Anbieter: Versand aller Arten von E-Mails der Flexopus Plattform; ausgenommen TKG-Dienstleistungen, insbesondere Senden, Übertragen und Empfangen des Kommunikationsinhalts
4	HubSpot Germany GmbH	Am Postbahnhof 17 10243 Berlin Deutschland	EU	Softwareanbieter für Vertrieb-, Marketing-, und Supportprozesse.
5	Banauten GmbH	Schlosserstr. 2 70180 Stuttgart Deutschland	EU	Service and Support, Vertrieb und Marketing
6	apicore engineering GmbH	Lise-Meitner-Str. 51 88046 Friedrichshafen Deutschland	EU	Support sowie Betrieb- und Wartungsanbieter