Datenschutzvereinbarung zur Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DS-GVO

zwischen dem Verantwortlichen:

_____ **← Firmenname**

_____ **← Straße, Hausnummer**

_____ **← Postleitzahl, Ort**

*(nachstehend **Auftraggeber** genannt)*

und dem Auftragsverarbeiter:

EDIT Systems GmbH
Gärtnerstraße 40
45128 Essen

*(nachstehend **Auftragnehmer** genannt)*

Haftungshinweis

Der nachfolgende AV-Vertrag wurde von den Verfassern auf Basis der aktuell verfügbaren Literatur erstellt. Dieser dient als erstes Muster. Es wird darauf hingewiesen, dass viele der angesprochenen Probleme noch nicht abschließend durch höchstrichterliche Rechtsprechung geklärt wurden und auch noch keine Stellungnahmen der Landesdatenschutzbehörden vorliegen, weshalb zu einigen Punkten noch unterschiedliche Auffassungen vertreten werden. Es wird keine Haftung auf Richtigkeit und Vollständigkeit übernommen. Ferner ist darauf hinzuweisen, dass jeder Fall gesondert zu prüfen ist und dieses Muster keine individuelle Rechtsberatung ersetzt.

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in dieser Vereinbarung beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Dienstleistung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Den Parteien ist bekannt, dass ab dem 25.05.2018 die EU Datenschutz-Grundverordnung (DS-GVO: EU-Verordnung 2016/679) gilt und sich die Vorgaben der Auftragsverarbeitung grundsätzlich nach Art. 28 DS-GVO richten.

Einzelvereinbarungen in dieser Datenschutzvereinbarung gehen den Allgemeinen Geschäftsbedingungen (AGB) des Auftragnehmers vor.

§ 1 Definitionen

1. **Personenbezogene Daten**
   Nach Art. 4 Abs. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden **"betroffene Person"**) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. **Auftragsverarbeiter**
   Nach Art. 4 Abs. 8 DS-GVO ist ein **Auftragsverarbeiter** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

3. **Weisung**
   Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Speicherung, Pseudonymisierung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete, in der Regel schriftliche Anordnung des Auftraggebers. Die Weisungen werden vom Auftraggeber erteilt und können durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers personenbezogene Daten oder es kann im Zusammenhang mit der Dienstleistungserbringung nicht ausgeschlossen werden, dass der Auftragnehmer Zugriff auf personenbezogenen Daten bekommt bzw. Kenntnis von diesen

erlangt. Nach Art 28 DS-GVO ist daher der Abschluss einer Vereinbarung zur Verarbeitung im Auftrag erforderlich.

2. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DS-GVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich bzw. auch elektronisch erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den Auftrag zur Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 DS-GVO und regelt die Rechte und Pflichten der Parteien zum Datenschutz im Zusammenhang mit der Erbringung der Dienstleistung.

3. Das Eigentum an den personenbezogenen Daten liegt ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

§ 3 Gegenstand und Dauer des Auftrages

1. Der Auftragnehmer erbringt für den Auftraggeber verschiedene Leistungen im Rahmen des „Cloud-Dienstleistungsvertrages“. Diese Leistungen beziehen sich auf das cloudbasierte ERP-System reybex, das für den professionellen Online- und Offline-Vertrieb von Handelswaren, die vollständige Auftragsabwicklung einschließlich der ordnungsgemäßen finanzbuchhalterischen Dokumentation der Geschäftsprozesse eingesetzt wird. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten und Rechte des Auftraggebers und des Auftragnehmers im Zusammenhang mit der Verarbeitung der personenbezogenen Daten des Auftraggebers durch den Auftragnehmer.
2. Diese Vereinbarung tritt mit ihrer Unterzeichnung durch beide Parteien in Kraft und endet im Regelfall mit Kündigung des zugrundeliegenden Hauptvertrages laut AGB. Das Recht zur außerordentlichen Kündigung bleibt unberührt.
3. Art und Zweck der Datenverarbeitung richten sich nach den getroffenen Vereinbarungen bzw. nach en Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser zugestimmt hat (mind. in Textform).
4. Folgende Datenarten sind von der Datenverarbeitung betroffen:
   <u>(ggf. durch Auftraggeber zu ergänzen)</u>
   - ◯ Kommunikationsdaten (z.B. Telefon, E-Mail)
   - ◯ Zahlungsarten (z.B. IBAN)
   - ◯ Kundendaten
   - ◯ Nutzerdaten (z.B. Name)
   - ◯ Bankdaten
   - ◯ Mitarbeiterdaten
   - ◯ …….
   - ◯ …….
   - ◯ …….
   - ◯ …….

5. Die von der Datenverarbeitung Betroffenen sind:
   (ggf. durch Auftraggeber zu ergänzen)
   - ◯ Mitarbeiter
   - ◯ Kunden
   - ◯ Interessenten
   - ◯ Lieferanten
   - ◯ Bewerber
   - ◯ Ansprechpartner
   - ◯ Dritte
   - ◯ …….
   - ◯ …….
   - ◯ …….
   - ◯ …….

§ 4 Technische und organisatorische Maßnahmen zum Datenschutz

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Wahrung der anzuwendenden Datenschutzvorschriften angemessen und erforderlich sind.

1. Da der Auftragnehmer die Dienstleistungen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt, sind vom Auftragnehmer zwingend die von ihm getroffenen technischen und organisatorischen Maßnahmen i.S.d. Art. 28 Abs. 3 lit. C DS-GVO, Art. 32 DS-GVO i.V.m. Art. 5 Abs. 1 und Abs. 2 DS-GVO hierzu zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben.

2. Die Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der mit diesem Auftrag in Zusammenhang stehenden Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und 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.

3. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage A „Technische und organisatorische Maßnahmen zum Datenschutz“** dieser Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

§ 5 Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber zur Erledigung durch diesen weiterleiten.

2. Die Umsetzung der Rechte auf Löschung, Berichtigung, Datenübertragbarkeit und Auskunft sind nur nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

3. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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 oder aufgrund gerichtlicher oder behördlicher Anordnung erforderlich sind.

4. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer dem Auftraggeber die Möglichkeit zum Zugriff und zur Sicherung sämtlicher in seinen Besitz gelangter Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, einzuräumen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

5. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 6 Pflichten des Auftragnehmers

1. Eine Verarbeitung personenbezogener Daten, die sich nicht auf die Erbringung der beauftragten Leistung bezieht, ist dem Auftragnehmer untersagt. Es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

2. Der Auftragnehmer bestätigt, dass er – soweit dieser gesetzlich dazu verpflichtet ist – einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 38, 39 DS-GVO bestellt hat.
   Die Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt. Auf Anforderung teilt der Auftragnehmer dem Auftraggeber den Namen und die Kontaktdaten des Datenschutzbeauftragten mit.

3. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt.

Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

4. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Auftraggebers.

5. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete personenbezogene Daten einer Verletzung des gesetzlichen Schutzes personenbezogener Daten gem. Art. 33 DS-GVO (Datenschutzverstoß bzw. Datenpanne) unterliegen, z.B. indem diese unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls bzw. der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Meldung an den Auftraggeber muss mindestens folgende Informationen 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 ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

    Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

6. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO notwendigen Angaben zur Verfügung und führt als Auftragsverarbeiter selbst ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO.

7. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zur Wahrung der Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugriff auf personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.

8. Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

9. Des Weiteren verpflichtet sich der Auftragnehmer den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Einhaltung der in Art. 34 - 36 DS-GVO genannten Pflichten zu unterstützen:

    a. Im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen und dem Auftraggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
    b. Bei der Durchführung seiner Datenschutz-Folgenabschätzung.
    c. Im Rahmen einer vorherigen Konsultation mit der Aufsichtsbehörde.

10. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

11. Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. Eine Information erfolgt nicht, soweit dies gerichtlich oder behördlich untersagt ist.

12. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung durch den Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

13. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

§ 7 Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren Auftragsverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können

    a. schriftlich
    b. per Fax
    c. per E-Mail
    d. mündlich

    erfolgen. Der Auftraggeber soll mündliche Weisungen unverzüglich in Textform (z.B. Fax oder E-Mail) gegenüber dem Auftragnehmer bestätigen.

2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3. Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 DS-GVO resultierenden Meldepflichten.

4. Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten personenbezogenen Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

5. Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 8 Wahrung von Rechten der betroffenen Person

1. Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Person verantwortlich.

2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung, Datenübertragbarkeit oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Löschung oder Einschränkung oder Datenübertragbarkeit seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

§ 9 Kontrollbefugnisse

1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Abs. 1 erforderlich ist.

3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Abs. 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur

im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

4. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

5. Der Auftragnehmer erbringt den Nachweis technischer und organisatorischer Maßnahmen, die nicht nur den konkreten Auftrag betreffen. Dabei kann dies erfolgen durch:

    a. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO.
    b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO.
    c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, Datenschutzauditoren.
    d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001).

6. Die Kosten für Aufwände einer Kontrolle beim Auftragnehmer gem. Abs. 3 und 4 können gegenüber dem Auftraggeber geltend gemacht werden.

§ 10 Unterauftragsverhältnisse

1. Die bedarfsweise Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.

2. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen Unternehmen zur Leistungserfüllung heranzieht bzw. mit Leistungen unterbeauftragt. Die zum Zeitpunkt des Abschlusses dieser Vereinbarung eingesetzten Unterauftragnehmer sind:

    - **Hosting**
      Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4-6, 32339 Espelkamp (Deutschland), Kontakt zum Datenschutzbeauftragten: datenschutz@mittwald.de

    - **Rechenzentrum**
      KAMP Netzwerkdienste GmbH, Vestische Str. 89-91, 46117 Oberhausen (Deutschland), Kontakt zum Datenschutzbeauftragten: luerweg@lundb.de

    - **Finanzen**
      finAPI GmbH, Adams-Lehmann-Str. 44, 80797 München (Deutschland), Kontakt zum Datenschutzbeauftragten: datenschutz@finapi.io

PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg (Luxemburg), Kontakt zum Datenschutzbeauftragten: PayPal (Europe) S.à r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxemburg

- **Live-Chat**
  INTERCOM, INC., 55 2nd St, 4th Fl., San Francisco, CA 94105 (USA), Kontakt zum Datenschutzbeauftragten: team@intercom.com

- **Logistik**
  DPD Deutschland GmbH, Wailandtstraße 1, 63741 Aschaffenburg (Deutschland), Kontakt zum Datenschutzbeauftragten: datenschutz@dpd.de

  General Logistics Systems, Germany GmbH & Co. OHG, GLS Germany-Straße 1 – 7, 36286 Neuenstein (Deutschland)

  DHL Paket GmbH, Sträßchensweg 10, 53113 Bonn (Deutschland), Kontakt zur Datenschutzbeauftragten: Gabriela Krader, LL.M, Deutsche Post AG, 53250 Bonn

  DHL Freight GmbH, Godesberger Allee 102-104, 53175 Bonn (Deutschland), Kontakt zur Datenschutzbeauftragten: Gabriela Krader, LL.M, Deutsche Post AG, 53250 Bonn

  United Parcel Service Deutschland S.à r.l. & Co. OHG, Görlitzer Straße 1
  41460 Neuss (Deutschland), Kontakt zum Datenschutzbeauftragten: UPS Europa SA Datenschutzbehörde, Ave Ariane 5, Brüssel, B-1200, Belgien

3. Im Falle einer Beauftragung hat der Auftragnehmer den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37-39 DS-GVO bestellt hat.

4. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

5. Die Verpflichtung des Unterauftragnehmers muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

6. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 10 dieser Vereinbarung) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

7. Nicht als Unterauftragsverhältnisse zu benennen sind Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Erfüllung der geschäftlichen Tätigkeit in Anspruch nimmt. Dazu zählen Reinigungsleistungen, Postdienste, Telekommunikationsleistungen und Bewachungsdienste. Der Auftragnehmer ist jedoch verpflichtet, auch bei diesen Diensten geeignete Vorkehrungen zum Schutz personenbezogener Daten zu treffen. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DS-GVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

§ 11 Datengeheimnis und Geheimhaltungspflichten

1. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist.

3. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieser Vereinbarung erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den oben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

4. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 12 Haftung

1. Es wird auf die Haftungsregelungen des Art. 82 DS-GVO verwiesen.

§ 13 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DS-GVO liegen.

2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei Unwirksamkeit einer Bestimmung in diesen Vertragsbedingungen bleiben die übrigen Bestimmungen gleichwohl wirksam. Die Vertragsparteien verpflichten sich, eine unwirksame Bestimmung oder eine planwidrig fehlende Bestimmung nach Treu und Glauben durch eine Bestimmung zu ersetzen, die dem gemeinsam verfolgten Zweck der Vertragsparteien am nächsten kommt.

Ort, ____.____.2018 Essen, ____.____.2018

Auftraggeber EDIT Systems GmbH

Anlage:

Technische und organisatorische Maßnahmen zum Datenschutz

Technische und organisatorische Maßnahmen zum Datenschutz

gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation der Vergabe von Schüsseln oder RFID-Chipkarten
Gesonderte Zutrittskontrolle für Räume mit kritischer IT-Infrastruktur
Rückgabe von Schüsseln oder RFID-Chipkarten nach Austritt von Mitarbeitern
Schutz des Firmengeländes (Pforte, Zaun etc.)
Verwendung einer Alarmanlage
Verwendung einer Video-Überwachung (Firmengelände, Eingangsbereich)
Verwendung einer Zutrittskontrolle (schlüsselbasierte oder RFID-basierte Zutrittssysteme)
Manuelles Schließsystem
Sicherheitsschlösser
Schlüsselregelung (Schlüsselausgabe etc.)
Protokollierung der Besucher
Vor Beendigung des Anstellungsverhältnisses müssen Mitarbeiter zuvor ausgehändigte Schlüssel, RFID-Chipkarten oder -Transponder zurückgeben

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten (z. B. Festplatten, Server)
Automatisches Sperren von PCs/Macs nach x Minuten
Verwendung personalisierter Logins im Unternehmensnetzwerk
Verwendung sicherer und individueller Passwörter
Zwei-Faktor-Authentifizierung (z. B. mittels Yubikey)
Einsatz einer Hardware-Firewall

Einsatz einer Software-Firewall
Einsatz von Anti-Viren-Software
Verschlüsselung von mobilen Datenträgern
Einsatz von VPN-Technologie
Sperren von externen Schnittstellen (USB etc.)
Tägliches Aufräumen der Arbeitsplätze ("Clean desk”)

1.3 Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation eingerichteter Zugänge für Mitarbeiter
Einführung von Benutzer- und Rollenkonzepten für interne Systeme
Sicherung von Schnittstellen (USB, LAN etc.) an öffentlich zugänglichen IT-Systemen
Sperrung von Zugängen nach Austritt von Mitarbeitern
Zentrale Verwaltung von Benutzerzugängen und -rechten
physische Löschung von Datenträgern vor Wiederverwendung
ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
Verschlüsselung von Datenträgern
Sichere Aufbewahrung von Datenträgern
Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

Nutzung SSL-verschlüsselter Übertragungswege im Internet
Sicherung von Dokumenten beim Versand auf dem Postweg (z. B. undurchsichtige Versandhüllen)
Verschlüsselter Versand von E-Mails (S/MIME, PGP)
Verwendung digitaler Signaturen für Dateien und E-Mails
Verwendung von VPN-Systemen zum Login in das Firmennetzwerk

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Mandantenfähigkeit von bereitgestellten Anwendungen
Einführung von Zugriffsberechtigungen für interne Systeme
Trennung von internem WLAN und Gäste-WLAN
Trennung von Live-, Test- und Entwicklungssystemen
Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk
Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk

1.6 Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Trennung von Kontaktdaten und weiteren nutzerbezogenen Daten
Trennung von Kundenstammdaten und Auftragsdaten
Verwendung von Pseudonymen an Stelle von personenbezogenen Daten (z. B. IDs)
Verwendung verschlüsselter Übertragungswege für den Datenaustausch
Verwendung von Maßnahmen zur verschlüsselten Datenspeicherung
Verwendung von SSL-Zertifikaten oder HTTPS-Verbindungen für Hosting Umgebungen

1.7 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Durch den Auftragnehmer umgesetzte Maßnahmen:

Verwendung verschlüsselter Übertragungswege für den Datenaustausch
Verwendung von Maßnahmen zur verschlüsselten Datenspeicherung

Verwendung von SSL-Zertifikaten für Hosting Umgebungen

2. Integrität

2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Einführung von Benutzer- und Rollenkonzepten für interne Systeme
Einführung individueller Zugänge für interne Systeme
Protokollierung von Zugriffen im Firmennetzwerk
Verwendung personalisierter Logins im Unternehmensnetzwerk

2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Durchführung von Code-Reviews in der Entwicklung
Erstellung von Code-Dokumentationen in der Entwicklung
Klimatisierung von Räumen mit kritischer IT-Infrastruktur
Nutzung von Testverfahren (z. B. Unittests) in der Entwicklung
Nutzung einer Versionskontrolle (z. B. Git oder SVN) in der Entwicklung
Regelmäßige Aktualisierung der Virendefinitionen
Regelmäßige Durchführung von Datensicherungen
Regelmäßige Durchführung von Updates (Windows, Mac, Linux, Desktopanwendungen)
Regelmäßige Überprüfung der erstellten Datensicherungen
Verwendung einer Brandmeldeanlage
Verwendung eines Diebstahlschutzes für öffentlich zugängliche IT-Systeme (z. B. Kensington-Lock)

Verwendung einer Firewall (z. B. Barracuda, Check Point, Cisco, Sophos)
Verwendung eines Intrusion Detection Systems (z. B. Barracuda, Check Point, Cisco, Sophos)
Verwendung eines Virenscanners (z. B. AVG, Bitdefender, Emsisoft, ESET, Kaspersky, Symantec)
Verwendung einer unterbrechungsfreien Stromversorgung (USV) für interne Systeme
Verwendung eines Überspannungsschutzes für interne Systeme
Verwendung von RAID-Systemen (z. B. für lokale File- und Entwicklungsserver)
Erstellen eines Backup- & Recoverykonzepts

3.2 Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Durch den Auftragsnehmer umgesetzte Maßnahmen:

Dokumentation und Test von Datenwiederherstellungen
Erstellung von Notfallplänen zu kritischen Prozesse
Nutzung einer Versionskontrolle (z. B. Git oder SVN) in der Entwicklung
Regelmäßiger Testdurchlauf von Notfallplänen zu kritischen Prozesse

4. Weitere Maßnahmenbereiche

4.1 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation von datenschutzrelevanten Zwischenfällen
Durchführung von Penetrationstests
Durchführung von Security-Audits durch externe Sachverständige
Einsatz von Anwendungen zur Unterstützung datenschutzkonformer Prozesse (z. B. otris privacy)
Löschen nicht mehr benötigter Daten (z. B. veraltete Daten, Testumgebungen)
Sichere Entsorgung defekter/nicht mehr benötigter Hardware
Sichere Entsorgung von Dokumenten (z. B. Aktenvernichter, Reisswolf)
Zuteilung von datenschutzrelevanten Verantwortungsbereichen

4.2 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten
Beauftragung zertifizierter Dienstleister (z. B. TÜV-zertifiziertes Hosting)
Benennung eines Datenschutzbeauftragten (ab 10 Personen)
Beratung/Aufklärung der Kunden zum Thema Datenschutz
Durchführung von stichprobenartigen Überprüfungen bei Dienstleistern
Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
Regelmäßige Unterweisung und Fortbildung der Mitarbeiter zum Thema Datenschutz
Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Ort, _____._____.2018

Auftraggeber

Ort, _____._____.2018

Auftragnehmer/Dienstleister