Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen

[Firmenname inkl. Rechtsform]

[Firmenadresse]

- Verantwortlicher -
nachstehend **Auftraggeber** genannt

und der

Tidely GmbH

Chiemgaustr. 148

81549 München

- Auftragsverarbeiter -
nachstehend **Auftragnehmer** genannt

zusammen auch im Folgenden als die „**Parteien**“ bezeichnet.

Präambel

Dieser Vertrag zur Auftragsverarbeitung regelt die Rechte und Pflichten bezüglich der weisungsgebundenen Datenverarbeitung der Parteien im Rahmen der Leistungserbringung durch den Auftragnehmer. Der Auftraggeber hat den Auftragnehmer sorgfältig ausgewählt und insbesondere sichergestellt, dass der Auftragnehmer hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten durch ihn im Einklang mit den für ihn geltenden datenschutzrechtlichen Vorgaben erfolgt und den Schutz der Rechte der von der Verarbeitung betroffenen Personen gewährleistet.

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag ALLGEMEINE GESCHÄFTS- UND NUTZUNGSBEDINGUNGEN TIDELY GMBH vom Januar 2025, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

1.2. Ort der Verarbeitung durch den Auftragnehmer

Die Erbringung der vertraglich vereinbarten Datenverarbeitung kann auch außerhalb eines Mitgliedsstaates der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) stattfinden.

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Sollte für die Erbringung der vertraglich vereinbarten Datenverarbeitung eine Verlagerung in ein Drittstaat stattfinden, so wird das angemessene Schutzniveau in Drittstaaten (s. Anhang 2) wie folgt gewährleistet:

- durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO); oder
- durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO); oder
- durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO); oder
- durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DSGVO); oder
- durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO); oder
- durch sonstige Maßnahmen: […] Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DSGVO).

1.3. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

1.4. Der Auftraggeber kann diesen Vertrag als auch das zugrundeliegende Rechtsverhältnis nach Ziffer 1.1 jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will

oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

1.5. Die Beauftragung des Auftragnehmers entbindet den Auftraggeber nicht von seiner Verpflichtung, die für ihn geltenden datenschutzrechtlichen Vorgaben, insbesondere im Hinblick auf die Rechtmäßigkeit der Verarbeitung sowie der Wahrung der Rechte der betroffenen Personen (Art. 12 bis 22 DSGVO) zu wahren. Vor diesem Hintergrund bleibt der Auftraggeber für die Datenverarbeitung Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

2. Konkretisierung des Auftragsinhalts

2.1. Art der vorgesehenen Verarbeitung gem. Art. 4 Nr. 2 DSGVO

Im Rahmen der Auftragsverarbeitung sind folgende Arten von Verarbeitungen vorgesehen:

- Erheben
- Erfassen
- Organisation
- Ordnen
- Speicherung
- Anpassung oder Veränderung
- Auslesen
- Abfragen
- Verwendung
- Offenlegung durch Übermittlung
- Verbreitung oder eine andere Form der Bereitstellung
- Abgleich oder die Verknüpfung
- Löschen

2.2. Zweck der vorgesehenen Verarbeitung von Daten

Die Verarbeitung wird zu folgenden Zwecken durchgeführt:

- Durchführung der Registrierung und Verwendung der Daten, um die Services zur Verfügung zu stellen, Rechnungs-stellung und Verwaltung von Kunden-dateien; Verwaltung und Weiterverfolgung der Anfragen von Interessenten
- Zurverfügungstellung der Services
- Zahlungsmanagement

- Support über das Ticketsystem bei Anfragen / für Service

2.3. Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (Name, Anschrift)
- Kommunikationsdaten (Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten: Zahlungsflüsse, Rechnungsdaten, sonstige Zahlungsinformationen
- Bilddateien (Rechnungen)
- Login- und Nutzungsdaten wie IP-Adresse, Browserverlauf sowie Geräteinformationen, über die auf den Dienst zugegriffen wird, werden zur technischen Optimierung und Weiterentwicklung des Dienstes verarbeitet. Dies umfasst insbesondere die Verbesserung von Funktionalität, Stabilität und Ladegeschwindigkeit.

2.4. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden/Geschäftspartner des Auftraggebers
- Beschäftigte des Auftraggebers

3. Weisungsbefugnis des Auftraggebers

3.1. Der Auftragnehmer und jede von ihm zur Verarbeitung personenbezogener Daten befugte Person darf die im Auftrag verarbeiteten Daten nur nach dokumentierten Weisungen des Auftraggebers verarbeiten. Eine Verarbeitung für andere als in diesem Vertrag festgelegte Zwecke ist nicht gestattet.

3.2. Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Die Einzelweisungen sind vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

3.3. Soweit der Auftragnehmer der Auffassung ist, dass Weisungen gegen anwendbares Recht verstoßen, wird er den Auftraggeber hierüber unverzüglich informieren. In diesem Fall ist der Auftragnehmer berechtigt, die Umsetzung der Weisung so lange auszusetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Eine von den Weisungen des Auftraggebers abweichende Verarbeitung ist nur zulässig, sofern der Auftragnehmer durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4. Verpflichtung auf die Vertraulichkeit

Bei der Datenverarbeitung durch den Auftragnehmer ist es dessen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

5. Technische und organisatorische Maßnahmen (TOM)

5.1. Der Auftragnehmer hat seine innerbetriebliche Organisation so gestaltet, dass alle von ihm als Auftragsverarbeiter zu beachtenden, besonderen datenschutzrechtlichen Anforderungen gewahrt werden.

5.2. Er hat in diesem Zusammenhang insbesondere die in der Anlage 1 genannten technischen und organisatorischen Maßnahmen nach Art. 28 Abs. 3 lit. c, 32 DSGVO getroffen, die erforderlich sind, um die Anforderungen an die Sicherheit der Verarbeitung zu gewährleisten. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen wird der Auftragnehmer den Auftraggeber bestmöglich bei der Einhaltung der vom Auftraggeber zu treffenden technischen und organisatorischen Maßnahmen sowie dessen Pflichten nach Art. 32 DSGVO unterstützen.

5.3. Eine Aufstellung der von ihm getroffenen technischen und organisatorischen Maßnahmen hat der Auftragnehmer dem Auftraggeber vor Abschluss dieses Vertrages zur Prüfung übergeben.

5.4. Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Vor diesem Hintergrund ist es dem Auftragnehmer gestattet, neue Technologien oder technische Werkzeuge einzusetzen, mit denen der Schutz der von ihm verarbeiteten personenbezogenen Daten verbessert werden kann. Das Sicherheitsniveau der im Rahmen dieses Vertrags festgelegten Maßnahmen darf dabei jedenfalls nicht unterschritten werden.

5.5. Wesentliche Änderungen wird der Auftragnehmer dokumentieren und dem Auftraggeber in diesem Zusammenhang unaufgefordert in einer entsprechend angepassten Anlage vorlegen.

5.6. Auf Anfrage legt der Auftragnehmer geeignete Nachweise dafür vor, dass er alle erforderlichen technischen und organisatorischen Maßnahmen umgesetzt hat. Zum Nachweis der getroffenen technischen und organisatorischen Maßnahmen kann der Auftragnehmer aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung (z.B. nach Art. 42 DSGVO) durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

5.7. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate (auch Back-Ups) der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

5.8. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen

zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Pflichten des Auftragnehmers

6.1. Der Auftragnehmer gewährleistet die ordnungsgemäße Führung eines den Vorgaben des Art. 30 Abs. 2 DSGVO entsprechenden Verzeichnisses von Verarbeitungstätigkeiten.

6.2. An der Erstellung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

6.3. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn er der Auffassung ist, dass dieser Vertrag oder Teile davon nicht den Anforderungen an einen Vertrag zur Auftragsverarbeitung nach den relevanten Vorschriften der DSGVO und/oder etwaigen Leitlinien, Empfehlungen oder sonstigen Stellungnahmen der Aufsichtsbehörden, insbesondere der Datenschutzkonferenz, der ehem. Art. 29 Datenschutzgruppe oder des Europäischen Datenschutzausschusses entspricht. In einem solchen Fall werden sich die Parteien gemeinsam um die erforderlichen Anpassungen dieses Vertrages bemühen.

6.4. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden. Der Auftragnehmer wird alle in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.

6.5. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach diesem Absatz betroffen sind.

6.6. Soweit gesetzlich vorgeschrieben, hat der Auftragnehmer einen Datenschutzbeauftragten benannt oder wird einen Datenschutzbeauftragten benennen, der die ihm gem. Art. 38, 39 DSGVO obliegenden Aufgaben wahrnimmt. Die Kontaktdaten des Datenschutzbeauftragten hat der Auftragnehmer der für ihn zuständigen Datenschutz-Aufsichtsbehörde mitgeteilt. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz oder eine Erstbenennung ist dem Auftraggeber unverzüglich mitzuteilen.

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

7. Unterauftragsverhältnisse

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

7.2. Der Auftraggeber stimmt der Beauftragung der in der Anlage 2 aufgeführten Unterauftragnehmer unter den folgenden Bedingungen zu. Die Auslagerung auf Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, soweit der Auftragnehmer dies dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt.

7.3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7.4. Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragnehmern nachweisen.

7.5. Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen. Die Parteien halten klarstellend fest, dass der Auftragnehmer dem Auftraggeber stets für die Einhaltung der Pflichten des Unterauftragnehmers haftet. Im Falle einer Verletzung der Pflichten aus der Vereinbarung mit dem Auftragnehmer oder eines Verstoßes gegen relevante gesetzliche Vorgaben durch den Unterauftragnehmer bleibt der Auftragnehmer dem Auftraggeber voll verantwortlich.

8. Mobiles Arbeiten / Home-Office-Regelung

8.1. Der Auftragnehmer ist berechtigt, im Bedarfsfall seinen Beschäftigten, die mit der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers betraut sind, die Verarbeitung dieser Daten außerhalb der Betriebsräume (z. B. im Rahmen von Home-Office oder mobilem Arbeiten) zu gestatten. Die hierfür erforderliche Zustimmung gilt mit Unterzeichnung des Vertrages durch den Auftraggeber als erteilt.

8.2. Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch außerhalb seiner Betriebsräume gewährleistet ist. Abweichungen von einzelnen Maßnahmen bedürfen der vorherigen Abstimmung mit dem Auftraggeber und dessen Genehmigung in Textform.

8.3. Der Auftragnehmer stellt insbesondere sicher, dass bei der Verarbeitung personenbezogener Daten außerhalb der Betriebsräume (z. B. bei mobilem Arbeiten oder im Home-Office) die verwendeten Speicherorte so konfiguriert sind, dass eine lokale Speicherung auf den eingesetzten IT-Systemen ausgeschlossen ist. Sofern dies im Einzelfall nicht realisierbar ist, hat der Auftragnehmer sicherzustellen, dass die lokale Speicherung ausschließlich in verschlüsselter Form erfolgt und ein Zugriff durch im Haushalt lebende Personen oder sonstige Dritte ausgeschlossen ist.

8.4. Der Auftragnehmer ist verpflichtet, sicherzustellen, dass dem Auftraggeber eine wirksame Kontrolle, der im Rahmen des Auftrags erfolgenden Verarbeitung personenbezogener Daten im Home-Office möglich ist. Dabei sind die Persönlichkeitsrechte der betroffenen Beschäftigten sowie der weiteren im Haushalt lebenden Personen angemessen zu wahren

9. Unterstützungspflichten des Auftragnehmers

9.1. Der Auftragnehmer wird den Auftraggeber bestmöglich bei der Erfüllung seiner Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen (i. S. d. Art. 12–22 DSGVO) in Bezug auf ihre personenbezogenen Daten unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber unverzüglich insbesondere über alle Auskunfts-, Berichtigungs-, Lösch-, Einschränkungs- und Datenübertragungsverlangen betroffener Personen informieren. Entsprechende Anträge und Ersuchen wird der Auftragnehmer unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer ist nicht befugt betroffenen Personen oder Dritten Auskunft über die im Auftrag verarbeiteten personenbezogenen Daten zu geben.

9.3. Der Auftragnehmer wird den Auftraggeber bestmöglich bei der Erfüllung seiner gesetzlichen Verpflichtungen nach Art. 32 bis 36 DSGVO unterstützen. Soweit erforderlich, wird der Auftragnehmer in diesem Zusammenhang daher insbesondere

- ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen sicherstellen, 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,
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,

- den Auftraggeber im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung stellen,
- den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung unterstützen,
- den Auftraggeber im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde unterstützen.

9.4. Der Auftragnehmer wird den Auftraggeber unverzüglich über alle Kontrollhandlungen und Maßnahmen einer Datenschutz-Aufsichtsbehörde informieren. Dies gilt auch, wenn eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten beim Auftragnehmer ermittelt.

9.5. Soweit sich der Auftraggeber Kontrollen der Aufsichtsbehörden, einem Ordnungswidrigkeits- oder Strafverfahren, Ansprüchen einer betroffenen Person nach Art. 82 DSGVO, Ansprüchen eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt sieht, wird der Auftragnehmer den Auftraggeber hierbei bestmöglich unterstützen.

9.6. Die Parteien verpflichten sich, etwaige im Rahmen der Prüfung von Aufsichtsbehörden festgestellte und mit diesem Vertrag im Zusammenhang stehende Mängel unverzüglich zu beheben.

10. Berichtigung, Einschränkung und Löschung von Daten

10.1. Der Auftragnehmer wird von ihm verarbeitete personenbezogene Daten des Auftraggebers nur nach dessen Weisung berichtigen oder löschen. Soweit eine datenschutzkonforme Löschung oder Einschränkung der Datenverarbeitung nicht möglich ist, kann der Auftraggeber den Auftragnehmer mit der datenschutzkonformen Vernichtung von Datenträgern und sonstigen Materialien beauftragen. Wendet sich eine betroffene Person zwecks Berichtigung, Löschung ihrer personenbezogenen Daten oder Auskunft zu ihren personenbezogenen Daten unmittelbar an den Auftragnehmer, wird er dieses Gesuch unverzüglich an den Auftraggeber weiterleiten.

10.2. Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen und Datenträger sind nach DIN 66399 zu vernichten.

10.3. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

10.4. Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig,

wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

11. Kontrollrechte des Auftraggebers

11.1. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

11.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

11.3. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

11.4. Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

11.5. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

12. Haftung

Die Haftung der Parteien richtet sich nach den Haftungsregelungen des Art. 82 DSGVO.

13. Schlussbestimmungen

8.1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

8.2. Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

8.3. Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

8.4. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand ist – soweit zulässig – der Sitz des Auftragnehmers.

Auftraggeber:	**Auftragnehmer:**
[Ort, aktuelles Datum]	München, [aktuelles Datum]
[Unterschrift Auftraggeber]	*[Niclas Storz]*

ANLAGE 1: Allgemeine technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 DSGVO

Der Auftragnehmer hat die nachfolgenden technischen und organisatorischen Maßnahmen getroffen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Sicherheitsschlösser	☒ Schlüsselregelung/Liste
☒ Schließsystem mit Codesperre	☒ Empfang/Rezeption/Pförtner
☒ Klingelanlage mit Kamera	☒ Besucher in Begleitung durch Mitarbeiter
☒ Videoüberwachung der Eingänge	☒ Sorgfalt bei Auswahl der Reinigungsdienste

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Virus-Software Clients	☒ Erstellen von Benutzerprofilen
☒ Firewall	☒ Richtlinie „Sicheres Passwort“
☒ Intrusion Detection Systeme	☒ Richtlinie „Löschen/Vernichten“
☒ Einsatz VPN bei Remote-Zugriffen	☒ Richtlinie „Clean desk“
☒ Verschlüsselung von Datenträgern	☒ Allg. Richtlinie Datenschutz und/oder Sicherheit
☒ Verschlüsselung Smartphones	☒ Anleitung „Manuelle Desktopsperre
☒ Automatische Desktopsperre	☒ Passwortvergabe: alphanummerischer Zeichensatz, Mindestlänge der Zeichen, Großbuchstabe zwingend, Sonderzeichen zwingend, Kleinbuchstabe
☒ Verschlüsselung von Notebooks/Tablet	
☒ Zweistufenauthentifizierung mittels Token	

Technische Maßnahmen

☒ WLAN-Verschlüsselung (WPA 2)

☒ Automatische Zugriffssperre auf IT-Systeme nach vergeblichen Anmeldeversuchen

☒ Sperrung bei wiederholten Fehleingaben hinsichtlich der Passwortkonventionen bei Erstellung eines Passworts

Zugriffskontrolle

Maßnahmen, um zu gewährleisten, 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, verändert oder entfernt werden können.

Technische Maßnahmen

☒ Login mit Benutzername + Passwort

☒ Physische Löschung von Datenträgern

☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen

☒ Verwalten von Benutzerberechtigungen

☒ Einsatz Berechtigungskonzepte

☒ Minimale Anzahl an Administratoren

☒ Verwaltung Benutzerrechte durch Administratoren

☒ Datenschutzkonforme Vernichtung von Datenträgern (Akten, Laufwerke etc.)

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Speicherung, Veränderung, Löschung, Übermittlung). Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen

☒ Trennung von Produktiv- und Testumgebung

☒ Mandantenfähigkeit relevanter Anwendungen

☒ Verwahrung von Pseudonymen und Zuordnungsdateien in getrennten und abgesicherten Systemen

☒ Verschlüsselung von Datensätzen, die zum selben Zweck verarbeitet werden

Organisatorische Maßnahmen

☒ Steuerung über Berechtigungskonzept

☒ Festlegung von Datenbankrechten

☒ Datensätze sind mit Zweckattributen versehen

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/ pseudonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Maßnahmen, um zu gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ E-Mail-Verschlüsselung	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Einsatz von VPN	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Protokollierung der Zugriffe und Abrufe	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können

Technische Maßnahmen

- ☒ Manuelle oder automatisierte Kontrolle der Protokolle

Organisatorische Maßnahmen

- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☒ Klare Zuständigkeiten für Löschungen

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen

- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Getrennte Partitionen für Betriebssysteme und Daten
- ☒ Serverraumüberwachung: Temperatur und Feuchtigkeit
- ☒ Serverraum klimatisiert
- ☒ USV
- ☒ RAID System / Festplattenspiegelung
- ☒ Videoüberwachung Serverraum
- ☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum
- ☒ Umsetzung eines ausreichenden Viren- und Firewallschutzes
- ☒ Einsatz von Sicherheitsupdates auf Systemen, auf denen personenbezogene Daten des Verantwortlichen verarbeitet werden

Organisatorische Maßnahmen

- ☒ Backup & Recovery-Konzept (ausformuliert)
- ☒ Kontrolle des Sicherungsvorgangs
- ☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ☒ Existenz eines Notfallplans (z. B. BSI IT-Grundschutz 100-4)
- ☒ Monatliche Prüfung der Belastbarkeit der IT-Systeme sowie automatische Prüfung der Belastbarkeit von IT-Systeme durch den Cloud-Anbieter AWS

Technische Maßnahmen

☒ Permanente Backups durch AWS im Rahmen einer geo-redundanten Absicherung bei AWS Irland unter Nutzung der 3-2-1- Regel bei Backups

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

Datenschutz-Maßnahmen

Technische Maßnahmen

☒ Software-Lösungen für Datenschutz-Management im Einsatz

☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung (z. B. Wiki, Intranet ...)

☒ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12

☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

Organisatorische Maßnahmen

☒ Interner/externer Datenschutzbeauftragter Name/Firma/Kontaktdaten

☒ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet

☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich

☒ Interner / externer Informationssicherheits-beauftragter Name/Firma Kontakt

☒ Jährliche alle Sicherheitseinstellungen durch Hacker-/ Penetrationstests überprüft

☒ Regelmäßige interne Überprüfung / Aktualisierung aller Datenschutzmaßnahmen

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen

☒ Einsatz von Firewall und regelmäßige Aktualisierung

☒ Einsatz von Spamfilter und regelmäßige Aktualisierung

☒ Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen

☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)

☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

☒ Einbindung von ☒ DSB und ☒ ISB in Sicherheitsvorfälle und Datenpannen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. via Ticketsystem
	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Auswahl des Auftragnehmers unter Sorgfalts-gesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

Technische Maßnahmen

Organisatorische Maßnahmen

- ☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- ☒ Regelung zum Einsatz weiterer Subunternehmer
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
- ☒ Vereinbarung von Vertragsstrafen mit Auftragsverarbeitern bei Verstößen gegen Weisungen

ANLAGE 2: Auflistung der bestehenden Unterauftragsverhältnisse im Rahmen der Auftragsverarbeitung (gemäß 7.2. des Vertrages)

Firma / Unternehmen	Anschrift / Land	Geeignete Garantien nach Art. 44 ff. DSGVO	Leistungsbeschreibung	An den Subunternehmer übertragene Daten
Amazon Web Services (Cloud Service Anbieter)	Eschborner Landstraße 100, 60489 Frankfurt am Main / bzw. One Burlington Plaza, Burlington Road, Dublin 4, D04 Rh96, Ireland	Für den Fall, dass Daten in die USA übermittelt werden: EU-U.S. Data Privacy Framework — Next Certification Due Date: 01/06/2026	Speicherung und Verarbeitung der Daten, um die Services zur Verfügung zu stellen	Alle bei der Registrierung und Nutzung der Services von Tidely anfallenden Daten
Chargebee (Abonnementverwaltung)	CHARGEBEE B.V., Piet Heinkade 55, 1019GM Amsterdam, Netherlands	Für den Fall, dass Daten in die USA übermittelt werden: EU-U.S. Data Privacy Framework — Next Certification Due Date: 07/14/2026	Verwaltung und Rechnungserstellung für die zur Verfügung gestellten Services	Vom Verantwortlichen bereitgestellte Rechnungs- und Kontaktdaten
finAPI GmbH (Schnittstellenanbieter)	finAPI GmbH, Adams-Lehmann-Str. 44, 80797 München	-	Einheitliche Schnittstelle zum Online-Abruf von Banking-Informationen	Vom Verantwortlichen bereitgestellte Konto- und Rechnungsdaten
BANKSapi Technology Finance (Schnittstellenanbieter)	BANKSapi Technology GmbH, Pettenkoferstr. 35, 80336 München	-	Einheitliche Schnittstelle zum Online-Abruf von EBICS-Banking-Informationen	Vom Verantwortlichen bereitgestellte Kontodaten
Windata konfipay (Schnittstellenanbieter)	windata GmbH, Weißgerberweg 11, 88239 Wangen im Allgäu, Deutschland	-	Einheitliche Schnittstelle zum Online-Abruf von EBICS-Banking-Informationen	Vom Verantwortlichen bereitgestellte Kontodaten
Salt Edge Finance (Schnittstellenanbieter)	150 Elgin Street, Floor 10, Ottawa, ON, K2P 1L4, Canada	Angemessenheitsbeschluss (CELEX:32002D0002)	Einheitliche Schnittstelle zum Online-Abruf von Banking-Informationen	Vom Verantwortlichen bereitgestellte Kontodaten

HubSpot (CRM-System)	HubSpot, Inc., Two Canal Park, Cambridge, MA 02141 USA	Für den Fall, dass Daten in die USA übermittelt werden: EU-U.S. Data Privacy Framework — Next Certification Due Date: 11/12/2025, Abschluss von SCC	Verwaltung und Bearbeitung von Kundenanfragen	Name, E-Mail-Adresse, Hintergrundinformationen über das Unternehmen des Anfragenden
Stripe Payments (Zahlungsdienstleister)	Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, Grand Canal Dock, Dublin D02 H210, Irland	Für den Fall, dass Daten in die USA übermittelt werden: EU-U.S. Data Privacy Framework — Next Certification Due Date: 10/08/2025, Abschluss der SCC	Abwicklung der Kundenzahlung für die erhaltenen Services	Vom Verantwortlichen bereitgestellte Zahlungsdaten

Stand 01/2026