VERTRAG

ÜBER

DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN
IM SINNE DES ART. 28 ABS. 3
DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 („DSGVO“)

ZWISCHEN

Kunde/Nutzer

- nachfolgend AUFTRAGGEBER (VERANTWORTLICHER) genannt -

UND

Fobi AI Germany GmbH

Walter-Gropius-Str. 15

80807 München, Deutschland

- nachfolgend AUFTRAGNEHMER (AUFTRAGSVERARBEITER) genannt -

Präambel

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich bei der Erbringung der beauftragten Leistung ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit der Leistung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte weitere Auftragsverarbeiter auftragsgegenständliche personenbezogene Daten („Daten“) im Auftrag des Auftraggebers im Sinne der Art. 4 Nr. 2 und 28 DSGVO verarbeiten („Auftragsverarbeitung“).

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1. Aus dem Hauptvertrag ergeben sich Gegenstand, Dauer, Art und Zweck der Auftragsverarbeitung sowie die Art der Daten und die Kategorien betroffener Personen. Soweit sich diese Spezifizierungen aus dem Hauptvertrag nicht ergeben, sind diese Angaben in **Nr. I der Anlage 1** zu diesem Vertrag aufgenommen. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen bedürfen der Schriftform oder eines dokumentierten elektronischen Formats.

1.2. Die in diesem Vertrag und dem Hauptvertrag vereinbarten Dienstleistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung von Dienstleistungen oder von Teilarbeiten dazu in ein Drittland („Verlagerung“) bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Europäischen Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Alle zu Beginn der Verarbeitung auf Basis dieser Grundsätze bereits vorgenommenen Verlagerungen sind in **Nr. II der Anlage 1** zu diesem Vertrag aufgenommen.

1.3. Die Laufzeit und Kündigungsmöglichkeit dieses Vertrages richtet sich nach dem Hauptvertrag, sofern sich aus den Bestimmungen dieses Vertrages nichts anderes ergibt.

Der Auftraggeber kann diesen Vertrag und den Hauptvertrag – soweit dieser die in diesem Vertrag näher konkretisierte Dienstleistung betrifft – jedoch jederzeit ohne Einhaltung einer Frist kündigen, (1) wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, oder (2) der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will, oder (3) 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. Die Kündigung hat schriftlich oder in einem dokumentierten elektronischen Format zu erfolgen (Sonderkündigungsrecht bei schweren Datenschutzverstößen).

2. Rechte und Pflichten des Auftragnehmers

2.1. Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlung von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

2.2. Vorbehaltlich des Art. 28 Abs. 3 Satz 2 lit. a DSGVO informiert der Auftragnehmer den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. In diesem Fall darf der Auftragnehmer die Umsetzung der Weisung so lange aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen und insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt.

2.4. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der Daten die Vertraulichkeit zu wahren und insbesondere alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung besteht auch nach Abschluss der Verarbeitung bzw. nach Beendigung des Vertrages fort. Der Auftragnehmer sichert insoweit zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet; Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

2.5. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

2.6. Der Auftragnehmer unterstützt den Auftraggeber in angemessener Weise bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten oder bei erforderlichen Datenschutz-Folgenabschätzungen des Auftraggebers (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

2.7. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen, Verstöße und Verletzungen datenschutzrechtlicher Bestimmungen oder der Vereinbarungen dieses Vertrages durch bei ihm beschäftigte Personen oder von ihm beteiligte Dritte. Dies gilt bereits beim Verdacht einer entsprechenden Störung und insbesondere im Hinblick auf mögliche Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert insoweit zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO darf der Auftragnehmer für den Auftraggeber nur nach vorheriger Weisung selbst durchführen. Er wird jedoch in jedem Falle unverzüglich alle erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen treffen und sich hierzu mit dem Auftraggeber absprechen.

2.8. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO für die Auftragsverarbeitung niedergelegten Pflichten zur Verfügung stellen und – grundsätzlich nach vorheriger Terminvereinbarung – Überprüfungen und Inspektionen, die vom Auftraggeber oder einem anderen, von diesem beauftragten Prüfer, durchgeführt werden, ermöglichen und zu ihnen beitragen (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Ergänzend hierzu gelten die Ziffern 3.3 und 6 dieses Vertrages.

2.9. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind und er die mit der Erbringung der Dienstleistung beschäftigten Personen vor Aufnahme der Verarbeitung mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht hat. Er verpflichtet sich, auch die für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Diese sind, sofern gegeben, in **Nr. III der Anlage 1** zu diesem Vertrag aufgenommen.

2.10. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen vor der Verarbeitung zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO) und diese Vertraulichkeits- bzw. Verschwiegenheitspflicht auch nach Beendigung des mit der zur Verarbeitung der Daten befugten Person geschlossenen Vertrages bzw. der Auftragsverarbeitung fortbesteht.

2.11. Der Auftragnehmer nennt dem Auftraggeber einen Ansprechpartner für im Rahmen dieses Vertrages anfallende Datenschutzfragen und als konkreten Weisungsempfänger auf Seiten des Auftragnehmers. Dieser (und der konkrete Weisungsberechtigte des Auftraggebers) ist in **Nr. IV der Anlage 1** zu diesem Vertrag zu nennen. Bei einem Wechsel oder einer längerfristigen Verhinderung einer der genannten Personen ist dem anderen Vertragspartner unverzüglich in Schriftform oder einem dokumentierten elektronischen Format ein Nachfolger bzw. Vertreter mitzuteilen.

Weisungen sind für ihre Geltungsdauer und anschließend noch für drei weitere, volle Kalenderjahre aufzubewahren.

2.12. Der Auftragnehmer hat Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt.

2.13. Sofern die gesetzlichen Voraussetzungen vorliegen hat der Auftragnehmer eine(n) Beauftragte(n) für den Datenschutz zu bestellen. Näheres hierzu, insbesondere die Kontaktdaten der oder des ggf. bestellen Beauftragten für den Datenschutz, ist in **Nr. V der Anlage 1** zu diesem Vertrag festgelegt. Jeder Wechsel in der Person der(s) Datenschutzbeauftragten sowie die Erfüllung der gesetzlichen Voraussetzungen und die daraus folgende Bestellung eines(s) Datenschutzbeauftragten ist dem Auftraggeber schriftlich oder in einem dokumentierten elektronischen Format mitzuteilen.

2.14. Nach der Beendigung der Auftragsverarbeitung sind sämtliche beim Auftragnehmer vorhandenen oder an Subunternehmen gelangte Daten, Datenträger, Unterlagen und sonstige Materialen sowie insbesondere alle Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers herauszugeben oder datenschutzgerecht zu löschen bzw. zu vernichten. Näheres hierzu ist in **Nr. VI der Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

3.1. Für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

3.2. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag und dem Hauptvertrag festgelegten Verpflichtungen zu überzeugen (vgl. Ziffer 2.8).

3.3. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer erforderlich sein, werden diese grundsätzlich zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorankündigung von wenigstens 28 Tagen durchgeführt. Im Falle einer Schutzverletzung i.S.d. Art. 4 Nr. 12 DSGVO und bei schwerwiegenden Vertragsverstößen können Inspektionen auch mit kürzerer Ankündigungsfrist durchgeführt werden. Der Auftragnehmer darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

3.4. Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.5. Der Auftraggeber nennt dem Auftragnehmer einen Ansprechpartner für im Rahmen dieses Vertrages anfallende Datenschutzfragen und als konkreten Weisungsberechtigten des Auftraggebers. Dieser (und der konkrete Weisungsempfänger auf Seiten des Auftragnehmers) ist in **Nr. IV der Anlage 1** zu diesem Vertrag zu nennen. Bei einem Wechsel oder einer längerfristigen Verhinderung einer der genannten Personen ist dem anderen Vertragspartner unverzüglich in Schriftform oder einem dokumentierten elektronischen Format ein Nachfolger bzw. Vertreter mitzuteilen.

3.6. Weisungen werden anfänglich durch den Hauptvertrag bzw. diesen Vertrag festgelegt. Spätere Weisungen sind grundsätzlich schriftlich oder in einem dokumentierten elektronischen Format an die vom Auftragnehmer bezeichnete Stelle (vgl. **Nr. IV der Anlage 1** zu diesem Vertrag) zu erteilen. Mündliche Weisungen sind für ihre Gültigkeit unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Weisungen sind für ihre Geltungsdauer und drei weitere Jahre, beginnend mit dem Ablauf des Kalenderjahres, in dem die Geltung der Weisung endet, aufzubewahren.

3.7. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Anfragen betroffener Personen

4.1. Im Falle der Inanspruchnahme einer der Parteien durch eine betroffene Person wegen etwaiger Ansprüche nach Art. 82 DSGVO sind der Auftragnehmer und der Auftraggeber verpflichtet sich gegenseitig bei der Abwehr des Anspruchs im Rahmen ihrer jeweiligen Möglichkeiten zu unterstützen.

4.2. Wendet sich eine betroffene Person mit einer Aufforderung zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen bzw. den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiterleiten, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Der Auftragnehmer ist nur nach vorheriger Zustimmung oder Weisung des Auftraggebers berechtigt, betroffenen Personen oder anderen Dritten Auskünfte über Daten, deren Verarbeitung oder das Auftragsverhältnis zu geben.

5. Technische und organisatorische Maßnahmen

5.1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Der Auftragnehmer wird alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung, insbesondere deren Art. 32 DSGVO genügen. Diese technischen und organisatorischen Maßnahmen („TOM“) sind diesem Vertrag als **Anlage 2** beigefügt. Sie beinhalten eine detaillierte Darstellung aller zum ermittelten Risiko passenden und unter Berücksichtigung der Schutzziele und der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer implementierten Maßnahmen. Der Auftragnehmer hat dabei insbesondere solche Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

5.2. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Die Maßnahmen beim Auftragnehmer oder einem beauftragten Subunternehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten sowie gesetzlich vorgesehenen Standards nicht unterschreiten. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen muss der Auftragnehmer mit dem Auftraggeber schriftlich oder in einem dokumentierten elektronischen Format abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages und für drei weitere Jahre, beginnend mit dem Ende des Kalenderjahres, in dem dieser Vertrag endet, aufzubewahren.

5.3. Der Auftragnehmer sichert zu, seinen Pflichten nach Art. 32 Abs. 1 lit. d DSGVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen. Die Ergebnisse sind dem Auftraggeber jeweils mitzuteilen.

6. Garantien, Nachweise

6.1. Der Auftragnehmer garantiert, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der Europäischen Datenschutz-Grundverordnung und diesem Vertrag erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet (Art. 28 Abs. 1 DSGVO). Er garantiert zudem, dass die durchgeführten technischen und organisatorischen Maßnahmen 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 ein angemessenes Schutzniveau gewährleisten (Art. 32 Abs. 1 DSGVO). Die Einhaltung dieser Garantien weist der Auftragnehmer dem Auftraggeber mit geeigneten Mitteln (z.B. Dokumente, Zertifikate, Audits, Testate etc.) nach. Näheres hierzu ist in **Nr. VII der Anlage 1** zu diesem Vertrag festgelegt.

6.2. Sofern einschlägig verpflichtet sich der Auftragnehmer, den Auftraggeber über den vorläufigen oder endgültigen Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers bedarf grundsätzlich entweder der gesonderten Zustimmung des Auftraggebers im Einzelfall oder der allgemeinen Genehmigung (Art. 28 Abs. 2 DSGVO). Der Auftragnehmer muss in jedem Falle dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem implementierten technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

7.2. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

7.3. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn kein Zugriff auf Daten des Auftraggebers erfolgen kann), Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die

Einbindung von Entsorgungsunternehmen ist jedoch anzeigepflichtig, wenn der Kern der Beauftragung die Entsorgung von Dokumenten/Datenträgern welche Daten des Auftraggebers enthalten, beinhaltet. Der Auftragnehmer wird jedoch auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen und erforderliche Kontrollmaßnahmen ergreifen, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

7.4. Bei Beauftragung von Subunternehmern hat der Auftragnehmer vertraglich sicherzustellen, dass die zwischen ihm und dem Auftraggeber vereinbarten Regelungen auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

7.5. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem dokumentierten elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

7.6. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

7.7. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

7.8. Die Entscheidungen darüber, ob Subunternehmer eingeschaltet werden dürfen und ggf. die dann folgende Verfahrensweise bei der Beauftragung von Subunternehmern ist in **Nr. IX der Anlage 1** zu diesem Vertrag geregelt.

7.9. Gegebenenfalls abweichend von den Festlegungen in **Nr. IX der Anlage 1** zu diesem Vertrag sind für den Auftragnehmer bereits bei Abschluss dieses Vertrages die in **Nr. VIII der Anlage 1** zu diesem Vertrag bezeichneten Subunternehmer mit der Verarbeitung von Daten in dem dort genannten Umfang beschäftigt. Insoweit sichert der Auftragnehmer zu, dass die in dieser Ziffer 7 genannten Voraussetzungen für die Beauftragung dieser Subunternehmer eingehalten worden sind. Vorbehaltlich der Vorlage der Prüfunterlagen gemäß Ziffer 5 dieses Vertrages, erklärt sich der Auftraggeber mit der Beauftragung der in der Anlage genannten Subunternehmer einverstanden.

8. Haftung und Schadensersatz

8.1. Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen, gegenüber betroffenen Personen insbesondere gemäß Art. 82 DSGVO.

8.2. Soweit der Auftraggeber wegen einer rechts- oder pflichtwidrigen Verarbeitung von Daten, die in den Verantwortungsbereich des Auftragnehmers oder eines von ihm beauftragten Dritten (Subunternehmer) fällt, in Anspruch genommen wird, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen Dritter frei.

9. Schlussbestimmungen

9.1. Soweit dieser Vertrag vor dem 25.05.2018 und damit vor Geltungserlangung der DSGVO abgeschlossen wurde, sind sich die Vertragsparteien einig, dass bis zu diesem Zeitpunkt das jeweils national geltende Datenschutzrecht entsprechend anzuwenden ist. Dies gilt insbesondere für solche Regelungen, die ausdrücklich auf die DSGVO verweisen.

9.2. Sollten die 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 und Beteiligten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

9.3. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.

9.4. Technische organisatorische Maßnahmen und jede Änderung zu diesen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmern) sind während der Laufzeit dieses Vertrages und für drei weitere Jahre, beginnend mit dem Ende des Kalenderjahres, in dem dieser Vertrag endet, aufzubewahren.

9.5. Mündliche Nebenabreden zu diesem Vertrag bzw. zu den mit diesem Vertrag geregelten Gegenständen wurden nicht getroffen. Gegebenenfalls bestehende, frühere mündliche Absprachen werden mit Zustandekommen dieses Vertrages aufgehoben.

9.6. Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen und Garantien des Auftraggebers – bedürfen einer schriftlichen Vereinbarung, die auch in einem dokumentierten elektronischen Format erfolgen kann, 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.

9.7. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages und seiner Anlagen den Regelungen des Hauptvertrages vor; die Anlagen dieses Vertrages gehen dem Vertrag vor.

9.8. Sollten einzelne Bestimmungen dieses Vertrages oder seiner Anlagen ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieses Vertrages und seiner Anlagen beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

9.9. Dieser Vertrag und seine Anlagen unterliegen dem Recht der Bundesrepublik Deutschland.

Dieser Vertrag wurde von beiden Seiten auf elektronischem Weg akzeptiert und ist daher auch ohne Unterschrift gültig.

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

I. ***zu Ziffer 1.1*** *- Umfang, Art und Zweck der Auftragsverarbeitung, Art der personenbezogenen Daten und Kreis der betroffenen Personen*

Gegenstand des Auftrags:

Erstellung, Versand und Verwaltung/Aktualisierung von digitalen Werbemitteln (Wallet Karten) für Smartphones.
Zur Verfügungstellung von Landingpages zum Verkauf und zur Erstellung von Wallet-Karten.

Umfang, Art und Zweck der Auftragsverarbeitung (beauftragte Leistungen):

-entsprechend der Definition von Art. 4 Nr. 2 DSGVO-

Digitale Werbemittel (Wallet Karten) können individualisierte Daten, wie z.B. Kundennamen, Kundennummern, ID's etc. enthalten. Darüber hinaus werden Logfiles mit Transaktionsdaten erzeugt und gespeichert. Welche personenbezogenen Daten enthalten sind, kann der Kunde selbst definieren. Sh. hierzu auch die gültigen AGB.

Datenarten, die verarbeitet werden:

-entsprechend der Definition von Art. 4 Nr. 1, 9, 13, 14 und 15 DSGVO-

☒ Personenstammdaten (z.B. Anrede, Name, Vorname, Adresse, Titel, Funktion)
☒ Kommunikationsdaten (Telefon, E-Mail)
☒ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse)
☒ Kundenhistorie (z.B. Käufe, Angebote, Anfragen, Kaufverhalten)
☒ Vertragsstamm-, Vertragsabrechnungs- und Zahlungsdaten
☒ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☒ Technische Protokolldaten (z.B. Login, IP, Zeitstempel)
☒ Daten, die Nutzer in Nachrichten, Freitextfeldern oder als Inhalt von Dateien von sich aus übermitteln:
Kontextuell bezogene Inhalte wie Werbeaussagen, Produktinformationen, Aufrufe, Wegbeschreibungen, Kontaktinformationen, URL's, Loyalitätsprogramm.
☐ Besondere personenbezogene Daten gem. Art. 9 Abs. 1 DSGVO (rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person):

☐ Weitere Daten:
Geo-Lokalisierung

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

Kreis der von der Datenverarbeitung betroffenen Personen:

-entsprechend der Definition von Art. 4 Nr. 1 DSGVO-

☒ Kunden des Auftraggebers
☒ Kunden von Kunden des Auftraggebers
☒ Beschäftigte des Auftraggebers
☒ Beschäftigte von Kunden des Auftraggebers
☒ Ansprechpartner von Lieferanten des Auftraggebers
☒ Ansprechpartner von Lieferanten von Kunden des Auftraggebers
☒ Interessenten des Auftraggebers
☒ Interessenten von Kunden des Auftraggebers
☐ Andere

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

***II. zu Ziffer 1.2** – Bestehende Verlagerungen der vertraglich vereinbarten Dienstleistung (oder Teilen) in ein Drittland:*

Dienstleistung / Verarbeitungsprozess	Angabe zum Drittland	Basis nach Art. 44 DSGVO
CRM-System (Hubspot 25 First Street, 2nd Floor Cambridge, MA 02141 United States)	*USA*	*Standardvertragsklauseln*
Support-System (Atlassian Pty Ltd 350 Bush Street Floor 13 San Francisco, CA, USA 94104)	*USA*	*Standardvertragsklauseln*
Functional Software, Inc. dba Sentry, 132 Hawthorne Street, San Francisco, CA 94107. USA	*USA*	*Standardvertragsklauseln*
IT-Sicherheit/DDoS-Schutz (Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107 USA)	*USA*	*Standardvertragsklauseln*
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland	*USA*	*Standardvertragsklauseln*
Fobi AI Inc. 541 Howe St #2F Vanouver, BC V6C 2C2 Canada	*Kanada*	*Angemessenheitsbeschluss der EU*

***III. zu Ziffer 2.9** – Für den Auftrag relevante Geheimnisschutzregeln:*
(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

IV. zu Ziffer 2.12 und Ziffer 3.5 – Weisungsbefugnis

Weisungsberechtigte Personen des Auftraggebers sind:

Kunde/Nutzer

Weisungsempfänger beim Auftragnehmer sind:

David Sporer, Geschäftsführer, +498925007997, privacy@passcreator.com

Für Weisung zu nutzende Kommunikationskanäle:

Walter-Gropius-Str. 15, 80807 München, privacy@passcreator.com, +498925007997

V. zu Ziffer 2.13 – Datenschutzbeauftragte(r)

☒ Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz bestellt

Karl Fröhlich
Zertifizierter Datenschutzbeauftragter
Ginsterweg 12
81377 München
Germany
Phone: +49 89 740 03 99
E-Mail: datenschutz@karlfroehlich.de
Web: www.karlfroehlich.de

☐ Ein(e) Datenschutzbeauftragte(r) ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung zum Zeitpunkt des Vertragsschlusses nicht vorliegt.

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

VI. zu Ziffer 2.14 – Löschpflichten

☒ Der Auftragnehmer wird jeweils direkt im Anschluss an einen erledigten Auftrag die im Rahmen dieses Einzelauftrages verarbeiteten Daten datenschutzgerecht löschen bzw. vernichten oder vernichten lassen.

☒ Nach Abschluss der vertraglichen Arbeiten bzw. bei Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen,

☒ dem Auftraggeber auszuhändigen, sofern relevant.

☒ wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen: Löschung der Dateien auf den Servern des Auftragnehmers.

Jede Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

VII. zu Ziffer 6 – Nachweise

☐ Ergebnisse eines Selbstaudits (vgl. Anlage *Nummer der Anlage)*.

☐ Zertifikat zu Datenschutz- und / oder Informationssicherheit (z.B. ISO 27001)

☐ Genehmigte Verhaltensregeln (Art. 40 DSGVO) einschließlich eines externen Nachweises über deren Einhaltung. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die genehmigten Verhaltensregeln nach Art. 40 DSGVO verwiesen. Diesen hat sich der Auftragnehmer am (Datum) unterworfen und deren Einhaltung am *(Datum)* geprüft und bestätigt wurden.

☐ verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO) einschließlich eines externen Nachweises über deren Einhaltung. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die verbindlichen internen Datenschutzvorschriften nach Art. 47 DSGVO verwiesen. Diesen hat sich der Auftragnehmer am (Datum) unterworfen und deren Einhaltung am geprüft und bestätigt wurde.

☐ Zertifikate gemäß Art. 42 DSGVO
Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit wird auf die vorliegende Zertifizierung nach Art. 42 DSGVO verwiesen, deren Einhaltung durch den Auftragnehmer am geprüft und bestätigt wurde.

☐ Auftraggeber und Auftragnehmer verständigen sich darauf, dass der erforderliche Nachweis auch durch folgende Unterlagen und Zertifikate erbracht werden kann:
Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf die vorliegende Zertifizierung durch die [Zertifizierungsstelle] verwiesen, deren Vorlage dem Auftraggeber für den Nachweis geeigneter Garantien ausreicht.

VIII. zu Ziffer 7.9 – Zu Beginn der Verarbeitung bereits beauftragte Subunternehmer:

Name und Adresse	Beschreibung der vom Subunternehmer erbrachten Leistungen
Flownative GmbH, Arnimstraße 19c, 23566 Lübeck	*Hosting*
SMSAPI ComVision sp. z o. o. ul. Toszecka 101 44-100 Gliwice Poland	*Versand von SMS*
Mailjet Mailjet SAS (Global HQ) 13-13 bis, rue de l'Aubrac, 75012 Paris, France	*Versand von E-Mails*
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland	*- Analyse von Zugriffen auf Websites (Google Analytics) - Übermittlung von Daten, die auf Wallet Karten für Google Pay dargestellt werden. - Nutzung von Google Cloud Diensten*
Hubspot 25 First Street, 2nd Floor Cambridge, MA 02141 United States	*CRM-System*
Atlassian Pty Ltd 350 Bush Street Floor 13 San Francisco, CA, USA 94104	*Support-System Wenn du ein Support Ticket erstellst, wird mindestens deine E-Mail-Adresse gespeichert. Daten von Endkunden werden nicht von Atlassian verarbeitet.*
FastBill GmbH Bockenheimer Anlage 15, 60322 Frankfurt am Main, Germany	*Buchhaltungssoftware*
Functional Software, Inc. dba Sentry, 132 Hawthorne Street, San Francisco, CA 94107. USA	*Error Tracking System*
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107 USA	*Sicherheitsdienste wie DDoS-Schutz, Web Application Firewalls und Performance-Optimierung*
Elasticsearch GmbH Fidicinstr. 12 10965 Berlin Deutschland	*Suchdienst*

Anlage 1

zum VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM SINNE DES ART. 28 ABS. 3 DER EUROPÄISCHEN DATENSCHUTZ-GRUNDVERORDNUNG 2016/679 (DSGVO)

Fobi AI Inc. *541 Howe St #2F* *Vanouver, BC V6C 2C2* *Canada*	*Produktsupport, Software-Entwicklung und Vertrieb*

IX. zu Ziffer 7 – Regelung zum Umgang mit Subunternehmern

☒ Der Auftraggeber genehmigt allgemein, dass der Auftragnehmer weitere bzw. andere Subunternehmer einbindet. Der Auftragnehmer hat den Auftraggeber aber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Subunternehmers schriftlich oder in einem dokumentierten elektronischen Format zu informieren. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund für den Einspruch vor und die Parteien erzielen keine einvernehmliche Lösung über das weitere Vorgehen, steht dem Auftraggeber ein fristloses Sonderkündigungsrecht hinsichtlich der gesamten Auftragsverarbeitung zu. Erfolgt innerhalb von 28 Tagen nach Übersendung der Anzeige kein Einspruch durch den Auftraggeber, gilt die Zustimmung zur Änderung als erteilt.

☐ Der Auftragnehmer hat vor jeder Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Subunternehmers die Zustimmung des Auftraggebers einzuholen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt und zusichert, dass die in Ziffer 6 Dieses Vertrages niedergelegten Grundsätze für die Einschaltung von Subunternehmern eingehalten wurden. Die Zustimmung ist nur wirksam, wenn sie in Schriftform oder einem dokumentierten elektronischen Format erfolgt; sie darf nur aus wichtigen datenschutzrechtlichen Gründen verweigert werden.

☐ Die Beauftragung von Subunternehmern sowie ggf. die Änderung bestehender, genehmigter Subunternehmerverhältnisse (**Nr. VIII dieser Anlage**) durch den Auftragnehmer zur Erbringung der im Vertrag vereinbarten Leistungen und Tätigkeiten ist unzulässig.

zu Ziffer 5 des Vertrages *– technische und organisatorische Maßnahmen*

Der Auftragnehmer hat zum Zeitpunkt des Abschlusses dieses Vertrages folgende technischen und organisatorischen Maßnahmen (TOMs) implementiert:

Einzelne Verarbeitungstätigkeiten

Bezeichnung Verarbeitungstätigkeit:	☒Onlineshop. ☒Website. ☒Marketingmaßnahmen. ☐Personalmanagement. ☐Finanzbuchhaltung. ☒Kommunikation (E-Mail, Messenger, etc.). ☐Sicherheitsmanagement. ☐Lieferantenverwaltung. ☒Kundenverwaltung. ☒Verarbeitung von Daten im Auftrag Dritter (z.B. als Dienstleister). ☐ _____
Beschreibung der Verarbeitungstätigkeit (1-2 Sätze)	Speicherung von Daten zum Zwecke der Nutzung und Abrechnung, sowie des Marketings für die Online-Software Passcreator. _
Art der Daten / Datenkategorien:	☒Bestandsdaten (Namen, Adressen). ☒Kontaktdaten (E-Mail, Telefonnummern, Fax, Messenger). ☒Inhaltsdaten (Texteingaben, Fotografien, Videos). ☒Vertragsdaten (Zeitpunkt, Inhalt, Zahlungsinformationen, Kundenkategorie, Bonitätsdaten). ☒Nutzungsdaten (Interessen, Besuchte Webseiten, Kaufverhalten, Zugriffszeiten). ☒Meta-/Kommunikationsdaten (Geräte-IDs, IP-Adressen, Standortdaten). ☐Beschäftigtenstammdaten (Namen, Adressen, Lohngruppe, Steuermerkmale). ☐Bewerberdaten (Namen, Kontaktdaten, Qualifikationen, Bewerbungsunterlagen). ☒ Daten zu Kundenbindungsprogrammen, _____
Besondere Datenkategorien:	☐ _____ (**Art. 9 DSGVO, z.B. Gesundheitsdaten, genetische und biometrische Daten, sexuelle Orientierung, politische, religiöse, Gewerkschaftszugehörigkeit, ethnische Herkunft, etc.).**
Kreis/Kategorie betroffener Personengruppen:	☒Kunden. ☒Nutzer, Websitebesucher. ☒Empfänger von Marketingmaßnahmen. ☒Lieferanten, Dienstleister, Partnerunternehmen und deren Mitarbeiter. ☒Mitarbeiter, Bewerber. ☐ _____
Quellen der Daten und Beschreibung der Erhebung, Übermittlung, etc.	☒Onlineformular. ☒Freiwillige Selbstangaben. ☐Öffentlich jedermann zugängliche Daten. ☐Mittels von Onlinetools/Verfahren ermittelte Daten. ☒Daten aus Kundendatenbanken

Art der Verarbeitung:	☒Elektronische Verarbeitung. ☐Verarbeitung in analogen Systemen (Aktenablage, etc.). ☐ _____
Zwecke der Datenverarbeitung:	☒Begründung, Durchführung und Beendigung von Kauf oder Dienstleistungsverträgen. ☐Begründung, Durchführung und Beendigung von Kauf oder Beschäftigungsverträgen. ☒Sicherheitsmaßnahmen. ☐Marktforschung. ☒Marketing und Werbezwecke. ☒ Loyalitätsprogramme_____
Rechtsgrundlagen der Verarbeitung:	☒Art 6 Abs. 1 a), Art. 7 DSGVO (Einwilligung). ☐**Art. 6 Abs. 1 lit. 1/b, § 26 BDSG-Neu / § 32 BDSG „Beschäftigungsverhältnis".** ☒ **Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).** ☐ **Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Pflichten).** ☒ **Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen).** ☐ _____
Empfänger intern:	☐Personalabteilung ☐Finanzbuchhaltung ☒Marketing/PR ☒IT ☐Lager ☒Geschäftsführung
Übermittlung/Offenlegung gegenüber Dritten & Zweck.	☒ **Banken zwecks Begleichung/Einziehung Zahlungsforderungen.** ☐ **Speditionsunternehmen zwecks Warenlieferung.** ☒ **Trackinganbieter zwecks Reichweitenanalyse und Onlinemarketing.** ☒ Hostinganbieter zwecks Datenverarbeitung
Weitergabe ins Drittland (außerhalb EU/EWR)	☐ _____ ☒ Siehe III.
Löschfristen	☒Löschung mit Vertragsbeendigung/ Kündigung. ☐6 J, gem. § 257 Abs. 1 HGB (Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Handelsbriefe, Buchungsbelege, etc.). ☒10 J, gem. § 147 Abs. 1 AO (Bücher, Aufzeichnungen, Lageberichte, Buchungsbelege, Handels- und Geschäftsbriefe, Für Besteuerung relevante Unterlagen, etc.). ☐ _____
Spezielle Sicherheitsmaßnahmen (wenn nicht bereits im Allg. Sicherheitskonzept)	☒ Siehe Allg. Sicherheitskonzept_____ ☐ _____

Wurden die Betroffenen in einer Datenschutzerklärung oder vergleichbar informiert (wie)?	☒Datenschutzerklärung. ☐Individuell (z.B. per E-Mail). ☐keine, Information, weil _____ ☐_____
Wurden Grundsätze Privacy by Design/ by Default beachtet?	– _____ ● Data at Rest – Daten werden verschlüsselt gespeichert, wenn sie nicht aufgerufen werden ● Transparenz der Daten für den Kunden – der Kunde hat jederzeit die Möglichkeit, nachzuvollziehen, welche Daten im System gespeichert sind und hat auch die Möglichkeit, diese zu löschen und zu verändern/korrigieren ● Verwendung sicherer Verschlüsselung von Passwörtern ● Strikte, logische Trennung von Daten zwischen Mandanten ● Regelmäßige Aktualisierung der eingesetzten Software (inklusive z.B. PHP-Frameworks, Webserver)
Liegt ein Fall des Art. 22 DSGVO Automatisierte Entscheidungen im Einzelfall einschließlich Profiling vor?	☐_____ (falls ja, bitte beschreiben)
DS-Folgenabschätzung erforderlich?	☒ nein, weil kein erhöhtes Risiko. ☐ ja, weil _____
Anmerkungen/ Sonstiges	_____

Sicherheitskonzept

Datenschutz auf Mitarbeiterebene	☒Vertrauens-/Verschwiegenheitsverpflichtung. ☒Regelung BYOD. ☒Regelung Homeoffice. ☒Regelung betrieblicher Internet/E-Mail-Nutzung. ☒Schulungen. ☐_____
Archivierung, Löschung, Entsorgung und Einschränkung Verarbeitung	☒Es liegt ein Archivierungs-, Lösch- und Entsorgungskonzept mit festgelegten Zuständigkeiten vor. ☒ Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und Vorgaben für Geräteentsorgung und Entsorgungsdienstleister unterrichtet. ☐_____
Wahrung der Betroffenenrechte	☒Es liegt ein Konzept, das die Wahrung der Rechte der Betroffenen (Auskunft, Korrektur, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet, vor. ☐ _____
Notfallkonzept	☒Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. ☐ _____
Zutrittskontrolle	☐ Haustürschlösser. ☐ Zutrittsregelungen für betriebsfremde Personen ☒ Chipkarten-/Transponder-Schließsystem. ☐ Sicherheitsschlösser. ☐ Fenstersicherung. ☐ Videoüberwachung. ☐ Beaufsichtigung von Hilfskräften. ☐ _____ ☐ _____

Zugangskontrolle / Zugriffskontrolle	☒Firewalls (Hardware/Software). ☒Stets aktueller Virenschutz. ☒Stets aktuelle Softwareversionen. ☒Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten Zugriffsregulierungen. ☒Mindestpasswortlängen und Passwortmanager. ☐Einsatz von VPN-Technologie. ☐Sperren von externen Schnittstellen (USB etc.). ☒Einsatz von Intrusion-Detection-Systemen. ☒Verschlüsselung von mobilen Datenträgern und GerätenVerschlüsselung von mobilen Datenträgern und Geräten ☐Einsatz von zentraler Smartphone-Administrations-Software. ☒Protokollierung von Zugriffen auf Daten ☒Ordnungsgemäße Vernichtung von Datenträgern. ☐ _____ ☐ _____
Weitergabekontrolle	☒ Festlegung und Dokumentation der Empfänger. ☐ Pseudonymisierung. ☒ Verschlüsselung von Datenträgern und Verbindungen. ☐ Dedizierte Weitergabeberechtigungen. ☒ Die Mitarbeiter haben sich schriftlich verpflichtet, Daten nicht weiterzugeben, es sei denn dies ist zur Erfüllung von Anfragen von Ermittlungsbehörden nach Vorlage einer gesetzlichen Grundlage notwendig. ☐ _____
Eingabekontrolle	☒Protokollierung von Dateneingaben-, Änderungen und Löschungen. ☐Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind. ☒Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts. ☐ _____ ☐ _____
Auftragskontrolle	☒Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten. ☒Schriftliche Festlegung der Weisungen. ☒Kontrolle der Einhaltung bei Auftragnehmern. ☒Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags. ☐ _____ ☐ _____
Verfügbarkeitskontrolle/ Integrität	☒Notfallkonzept. ☒Ständig kontrolliertes Backup- und Recoverykonzept. ☒Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten. ☒Durchführung von Belastbarkeitstests. ☐ _____ ☐ _____

Gewährleistung des Zweckbindungs-/Trennungsgebotes	☐Physische Mandantentrennung (hardwareseitig). ☒Logische Mandantentrennung (softwareseitig). ☒Trennung von Produktiv- und Testsystem. ☐Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten System. ☐ _____ ☐ _____