Fleetboard Logistics GmbH

Vereinbarung über die Auftragsverarbeitung

Bei Fragen oder Problemen helfen wir Ihnen gerne weiter!

Ihr Team der Fleetboard Logistics GmbH

Telefon: +49 (9381) / 71 69 5-0
E-Mail: help@fleetboard-logistics.com

mit

Fleetboard Logistics GmbH
Am Alten Bahnhof 8, 97332 Volkach

– als Auftragsverarbeiter –

KONTAKTDATEN AUFTRAGSVERARBEITER

Name	Fleetboard Logistics GmbH
Straße / Nr.	Am Alten Bahnhof 8
PLZ / Ort	97332 Volkach
Name des Datenschutzbeauftragten	Vertraulich
Tel.	+49 9381 71 778 - 59
E-Mail	flelo.datenschutz@eikona.de

§ 1 VEREINBARUNG ÜBER DIE AUFTRAGSVERARBEITUNG UND DIE GEWÄHRLEISTUNG DER SICHERHEIT DER VERARBEITUNG

1.1. Beschreibung des Auftrags

1.1.1. Gegenstand des Auftrags

Der Auftragnehmer stellt eine Portallösung für den Austausch von verschiedenen Dateien (Auftrags-, Tour- und Sendungsdaten) zwischen mehreren Nutzern zur Verfügung. Weiterhin bietet er über die CONIZI Plattform einen Konverterdienst an, in dem die vorgenannten Daten in die verschiedenen logistischen Standardformate umgewandelt werden können.

1.1.2. Dauer dieses Auftrags (Laufzeit)

Die Laufzeit des Auftrags orientiert sich am Hauptvertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter.

1.1.3. Die Art der verarbeiteten personenbezogenen Daten

Personenstammdaten (Namen von jur. und nat. Personen, Adressen, Ansprechpartner), Kommunikationsdaten (Telefon, Handy, E-Mail), Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse), Kundenhistorie, Planungs- und Steuerungsdaten, Tour- / Auftragsdaten (Text-, Dokumente, Bild und Videodaten), GPS-Daten (zu festgelegten Aktionen im Workflow-Manager), Informationen über Systemkonfigurationen und Kundenumgebungen.

1.1.4. Standorte der Verarbeitung

Die Verarbeitung personenbezogener Daten findet ausschließlich in der Bundesrepublik Deutschland statt. Eine Übermittlung in ein Drittland findet nicht statt.

1.1.5. Umfang, Art und Zweck der Verarbeitung personenbezogener Daten

Umfang, Art und Zweck der Datenverarbeitung ergeben sich aus dem Hauptvertrag und ggf. weiteren Einzelbeauftragungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter.

1.1.6. Die Kategorien der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen:

Kunden, Interessenten, Beschäftigte im Sinne des § 26 (8) BDSG, Lieferanten, Ansprechpartner.

1.2. Geheimhaltung

1.2.1. Der Auftragsverarbeiter verpflichtet sich alle Informationen, insbesondere technische und wirtschaftliche Informationen sowie Absichten, Erfahrungen, Erkenntnisse, Konstruktionen und Unterlagen, die ihm unter dieser Vereinbarung vom Verantwortlichen zugänglich gemacht werden, oder die er vom Verantwortlichen erhält, vertraulich zu behandeln, Dritten nicht zugänglich zu machen, vor dem Zugriff Dritter zu schützen, nur für Zwecke dieser Vereinbarung zu verwenden und nur an Mitarbeiter weiterzugeben, die zur Einhaltung der Vertraulichkeit verpflichtet sind, solange zwischen den Parteien nichts anderes schriftlich vereinbart worden ist.

1.2.2. Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen,

- die dem Auftragsverarbeiter nachweislich bereits vor Inkrafttreten dieser Vereinbarung bekannt waren,
- die der Auftragsverarbeiter nachweislich rechtmäßig von Dritten ohne Auferlegung einer Vertraulichkeitsverpflichtung erhält,
- die allgemein bekannt sind oder ohne Verstoß gegen die in dieser Vereinbarung enthaltenen Verpflichtungen allgemein bekannt werden,
- die der Auftragsverarbeiter nachweislich im Rahmen eigener unabhängiger Entwicklungen erarbeitet hat.

1.2.3. Sofern es sich bei dem Verantwortlichen um ein Finanzdienstleistungsunternehmen handelt, für das die Anforderungen des Bankgeheimnisses gelten, verpflichtet sich der Auftragsverarbeiter zur Einhaltung derselben Anforderungen.

1.2.4. Der Auftragsverarbeiter verpflichtet sich, seinen Mitarbeitern, die von diesen Informationen Kenntnis erhalten, die gleichen Verpflichtungen, wie sie vorstehend der Auftragsverarbeiter eingegangen ist, aufzuerlegen, sofern diese Mitarbeiter nicht bereits in gleichem Umfang durch die jeweiligen Arbeitsverträge zur Geheimhaltung verpflichtet sind.

1.2.5. Für den Fall der Mitteilung etwaiger schutzrechtsfähiger Ergebnisse behalten sich die Parteien alle Rechte hinsichtlich eventueller späterer Schutzrechte vor.

1.2.6. Die Vertraulichkeitsverpflichtungen hinsichtlich von Informationen, die während der Laufzeit zugänglich wurden, dauern bis 5 Jahre nach Ende der Laufzeit fort.

1.3. Weisungsbefugnis des Verwantwortlichen

1.3.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Für die Einhaltung der datenschutzrechtlichen Bestimmungen liegt die Verantwortung beim Verantwortlichen.

1.3.2. Bei der Verarbeitung personenbezogener Daten ist der Auftragsverarbeiter verpflichtet, ausschließlich den Weisungen des Verantwortlichen zu folgen. Die Weisung bedarf der Textform. Außerhalb von Weisungen darf der Auftragsverarbeiter die ihm zur Verarbeitung überlassenen Daten weder für seine eigenen Zwecke noch für Zwecke Dritter verwenden. Der Auftragsverarbeiter hat nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Sofern der Auftragsverarbeiter der Meinung ist, dass Weisungen des Verantwortlichen gegen geltende Datenschutzbestimmungen verstoßen, hat er den Verantwortlichen unverzüglich darüber zu informieren.

1.4. Pflichten des Auftragsverarbeiters

1.4.1. Der Auftragsverarbeiter wird den Verantwortlichen bei der Umsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Löschung, Recht auf Datenübertragbarkeit der über sie gespeicherten Daten unterstützen. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks der oben genannten Betroffenenrechte wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

1.4.2. Der Auftragsverarbeiter verpflichtet sich, seine mit der Verarbeitung von Daten des Verantwortlichen befassten Mitarbeiter im Datenschutz zu schulen und auf das Datengeheimnis (Einhaltung der Vertraulichkeit personenbezogener Daten) zu verpflichten.

1.4.3. Der Auftragsverarbeiter teilt dem Verantwortlichen die Kontaktdaten des/der Ansprechpartner für Datenschutz und Informationssicherheit mit. Soweit der Auftragsverarbeiter gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet ist, benennt er diesen schriftlich und teilt dem Verantwortlichen den Namen und Kontaktdaten mit.

1.4.4. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die für die Erfüllung von Meldepflichten, die Führung einer Verfahrensübersicht oder die Durchführung einer Datenschutzfolgenabschätzung notwendigen Informationen zur Verfügung.

1.4.5. Jede Vertragspartei haftet gegenüber der jeweils anderen Vertragspartei für Schäden aus schuldhaften Verstößen gegen die Regelungen dieser Vereinbarung sowie anwendbare Datenschutzvorschriften. Sofern beide Parteien ein Verschulden trifft, haften sie jeweils gemäß ihres Anteils des Verschuldens.

1.4.6. Der Verantwortliche kann jederzeit die Löschung der unter dieser Vereinbarung verarbeiteten Daten anweisen. Unabhängig hiervon ist der Auftragsverarbeiter verpflichtet, jederzeit auf Verlangen des Verantwortlichen die Daten in einem allgemein lesbaren Format herauszugeben. Nach Ende der Laufzeit dieser Vereinbarung hat der Auftragsverarbeiter die Verpflichtung, die unter dieser Vereinbarung verarbeiteten Daten des Verantwortlichen nach Wahl des Verantwortlichen in einem allgemein lesbaren Format zurückzugeben oder zu löschen. Im Fall der Löschung muss die Rekonstruktion der Daten ausgeschlossen sein. Der Auftragsverarbeiter wird die vollständige Rückgabe und Löschung der Daten, Vervielfältigungen, Speichermedien nachweisen und in Textform bestätigen.

Sofern der Auftragsverarbeiter aufgrund zwingender gesetzlicher Vorschriften die Löschung bestimmter Daten, bzw. Datenkategorien, nicht vornehmen darf, muss er dies dem Verantwortlichen mitteilen.

1.4.7. Im Falle, dass der Auftragsverarbeiter oder wesentliche Unternehmensteile des Auftragsverarbeiters von einem Dritten erworben werden, oder erwirbt ein Dritter die Aktienmehrheit oder die Mehrheit der Stimmrechte am Auftragsverarbeiter, ist der Verantwortliche berechtigt, diese Vereinbarung außerordentlich zu kündigen.

1.5. Einsatz von Subunternehmern

1.5.1. Schaltet der Auftragsverarbeiter Subunternehmer oder freie Mitarbeiter ein, so bedarf dies der vorherigen Zustimmung des Verantwortlichen in Textform. Die vertraglichen Vereinbarungen zwischen dem Auftragsverarbeiter und dem Subunternehmer oder freien Mitarbeiter sind durch den Auftragsverarbeiter so zu gestalten, dass sie den hier getroffenen Vereinbarungen zwischen Verantwortlichem und Auftragsverarbeiter entsprechen. Insbesondere ist durch den Auftragsverarbeiter sicherzustellen, dass der Verantwortliche Kontrollen gemäß Ziff. 1.7 dieser Vereinbarung auch bei Subunternehmern oder freien Mitarbeitern durchführen kann. Der Verantwortliche ist berechtigt, vom Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der Verpflichtungen gemäß dieser Vereinbarung – erforderlichenfalls auch durch Einsicht in die relevanten Vertragsdokumente - zu erhalten.

1.5.2. Für die unter Teil 3 dieser Vereinbarung aufgeführten Subunternehmer und die dort genannten Aufgabenbereiche gilt die Zustimmung des Verantwortlichen mit Abschluss dieser Vereinbarung als erteilt. Der Auftragsverarbeiter stellt sicher, dass diese Subunternehmer die technischen und organisatorischen Maßnahmen gemäß Teil 2 dieser Vereinbarung ebenso implementieren wie der Auftragsverarbeiter selbst.

1.5.3. Werden während der Laufzeit dieser Vereinbarung Subunternehmer ausgetauscht oder hinzugefügt, so bedarf dies der vorherigen Zustimmung des Verantwortlichen in Textform. Beabsichtigt der Auftragsverarbeiter die Hinzuziehung anderer Subunternehmer als in Teil 3 vereinbart, so meldet er dies der ihm bekannten Vertragsmanagementfunktion des Verantwortlichen über ggf. vorgesehene Kommunikationskanäle. Hilfsweise nimmt er die Meldung gegenüber dem auf S. 2 angegebenen fachlichen Ansprechpartner des Verantwortlichen vor. Im Falle der Zustimmung durch den Verantwortlichen aktualisiert der Auftragsverarbeiter die Übersicht in Teil 3 und stellt die aktualisierte Version des Teils 3 dem Verantwortlichen zur Verfügung. Diese Vereinbarung gilt sodann mit dem aktualisierten Teil 3 fort.

1.6. Sicherheit der Verarbeitung

1.6.1. Der Auftragsverarbeiter verpflichtet sich, alle Informationen und Daten des Verantwortlichen nach dem Stand der Technik zu jeder Zeit mit dem Risiko der Verarbeitung angemessenen technischen und organisatorischen Maßnahmen zu sichern. Dies beinhaltet insbesondere den Schutz vor unberechtigtem Zugriff, unberechtigter oder unbeabsichtigter Veränderung, Zerstörung oder Verlust, unerlaubter Übermittlung, anderweitiger unerlaubte Verarbeitung und sonstigem Missbrauch. Die Maßnahmen sind in Teil 2 dieser Vereinbarung umfassend darzustellen. Die Verpflichtung zum Schutz der Informationen und Daten des Verantwortlichen gilt unbeschadet der Ziffer 1.1.2 so lange, wie der Auftragsverarbeiter diese Daten und Informationen speichert oder auf sonstige Weise verarbeitet oder durch Subunternehmer verarbeiten lässt.

1.6.2. Der Auftragsverarbeiter muss ein Managementsystem für Informationssicherheit etablieren. Vor dem Hintergrund der Risiken muss der Auftagsverarbeiter die von Ihm zu treffenden Maßnahmen bestimmen, regelmäßig überprüfen und anpassen. Sowohl die Risiken als auch die getroffenen Maßnahmen sind vom Auftagsverarbeiter zu dokumentieren und nachzuweisen.

1.6.3. Auf Anfrage des Verantwortlichen stimmt der Auftragsverarbeiter die zu treffenden technischen und organisatorischen Maßnahmen mit dem zuständigen Informationssicherheitsbeauftragten des Verantwortlichen ab.

1.6.4. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um hinreichende technische und organisatorische Maßnahmen nachzuweisen. Darüber hinaus können Zertifizierungen des Informationssicherheits-Managementsystems wie nach ISO 27.001 oder ISO 27.001 auf der Basis von IT-Grundschutz als Faktor herangezogen werden, um die Nutzung von technischen und organisatorischen Maßnahmen nachzuweisen. Ein solcher Nachweis ersetzt aber nicht die Prüfung der Angemessenheit im Einzelfall. Wird ein solcher Nachweis als Faktor herangezogen, ist er dieser Vereinbarung beizufügen.

1.6.5. Der Auftragsverarbeiter darf Zugriffsberechtigungen auf die Daten des Verantwortlichen nur an eigene Mitarbeiter gemäß Berechtigungskonzept und in dem für die jeweilige Aufgabe im Zusammenhang mit der Ausführung dieser Vereinbarung erforderlichen Umfang vergeben. Die zugriffsberechtigten Personen oder Personengruppen sind dem Verantwortlichen auf Anfrage zu benennen. Der Auftragsverarbeiter verpflichtet sich, keinem Unbefugten die ihm zur Nutzung des Systems zugeteilten Zugriffsberechtigungen bekannt zu geben.

1.6.6. Wird dem Auftragsverarbeiter die Möglichkeit eingeräumt auf die IT-Systeme des Verantwortlichen oder dessen Auftragsverarbeiter zuzugreifen, so verpflichtet er sich, nur auf die für die Ausführung dieser Vereinbarung notwendigen Daten und Informationen zuzugreifen.

1.6.7. Der Auftragsverarbeiter hat die ihm bekannte Vertragsmanagementfunktion des Verantwortlichen über ggf. vorgesehene Kommunikationskanäle, hilfsweise den zuständigen Informationssicherheitsbeauftragten des Verantwortlichen, über wesentliche Änderungen der in Teil 2 beschriebenen technischen und organisatorischen Maßnahmen in Textform zu informieren. Bei einer absehbaren Minderung der Schutzwirkung ist vor der Änderung die Zustimmung des Verantwortlichen in Textform einzuholen.

1.7. Kontrollen

1.7.1. Der Verantwortliche oder dessen Beauftragter ist berechtigt, die Einhaltung der Anforderungen dieser Vereinbarung zu kontrollieren. Der Auftragsverarbeiter wird die gewünschten Auskünfte erteilen und auf Wunsch des Verantwortlichen einen Nachweis über die Umsetzung seiner Verpflichtungen durch Ausfüllen eines vom Verantwortlichen verwendeten Fragebogens oder durch schriftliche Bestätigung der Angemessenheit und Aktualität der in Teil 2 vereinbarten Maßnahmen innerhalb angemessener Zeit erbringen.

1.7.2. Dem Verantwortlichen oder dessen Beauftragten ist nach vorheriger Anmeldung zwecks Überprüfung der Umsetzung dieser Vereinbarung sowie der Angemessenheit der technischen und organisatorischen Sicherheitsmaßnahmen Zutritt zu den

Räumen und Zugriff auf IT-Systeme, in denen Daten des Verantwortlichen verarbeitet werden, zu gewähren.

1.7.3. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen von Aufsichtsbehörden, die in seinem Unternehmen oder der von ihm genutzten IT-Infrastruktur stattfinden und in deren Rahmen eine Verarbeitung von personenbezogenen Daten des Verantwortlichen stattfindet. Im Falle eines bevorstehenden Zugriffs auf Daten des Verantwortlichen im Rahmen einer Pfändung, einer Beschlagnahme, eines Ermittlungsverfahrens oder einer sonstigen behördlichen Maßnahme, die beim Auftragsverarbeiter durchgeführt wird, oder im Rahmen eines Insolvenzverfahrens oder anderer Maßnahmen Dritter, informiert der Auftragsverarbeiter den Verantwortlichen darüber unverzüglich.

1.7.4. Der Auftragsverarbeiter informiert im Zusammenhang mit Ziffer 1.7.3 alle anfragenden Stellen unverzüglich darüber, dass die Verfügungsgewalt über diese Daten beim Verantwortlichen liegt und wird ohne die Zustimmung des Verantwortlichen keine Daten an Dritte übermitteln oder diesen Zugriffe ermöglichen. Wird der Auftragsverarbeiter im Falle einer Kontrolle, eines Zugriffs oder anderer ergriffener Maßnahmen in Bezug auf die Daten des Verantwortlichen durch die zugriffsberechtigte Stelle zur Verschwiegenheit verpflichtet, so hat er die Sorgfaltspflicht im Namen des Verantwortlichen jede Möglichkeit zu ergreifen gegen die Maßnahmen und die Verschwiegenheitsverpflichtung vorzugehen.

1.8. Meldung von Datenschutz-Sicherheitsverletzungen

1.8.1. Der Auftragsverarbeiter hat den Verantwortlichen im Falle von Datenschutz-Sicherheitsverletzungen (unbeabsichtigte/r oder unbefugte/r Vernichtung, Verlust, Veränderung, Offenlegung oder Zugang bezüglich unter dieser Vereinbarung verarbeiteter personenbezogener Daten) oder bei Verletzung des Bankgeheimnisses unverzüglich zu informieren, um dem Verantwortlichen die Meldung des Vorfalls binnen 72 Stunden an die zuständige Aufsichtsbehörde zu ermöglichen.

1.8.2. In Abstimmung mit dem Verantwortlichen leitet der Auftragsverarbeiter unverzüglich alle erforderlichen Schritte zur Aufklärung des Sachverhalts und zum Abstellen der Datenschutz-Sicherheitsverletzung ein und stellt dem Verantwortlichen alle erforderlichen Informationen zur Dokumentation des Vorfalls und ggf. Durchführung der Meldung an die zuständige Aufsichtsbehörde zur Verfügung.

§ 2 Maßnahmen zur Gewährleistung der Sicherheit und der Verarbeitung

Im Folgenden sind die technischen und organisatorischen Maßnahmen zu dokumentieren, die vom Auftragsverarbeiter für die Gewährleistung der Sicherheit der Datenverarbeitung umgesetzt werden.

Die einzelnen technischen und organisatorischen Maßnahmen sind zur Übersichtlichkeit ihren primären Schutzzielen, der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten, zugeordnet. Organisatorische und prozessuale Schutzmaßnahmen unterstützen die primären Schutzziele.

Nicht alle im Folgenden aufgelisteten Maßnahmen sind umzusetzen; es ist jeweils ein in der Gesamtheit angemessener Schutz gemäß dem Stand der Technik durch den Auftragsverarbeiter zu gewährleisten. Beim Stand der Technik handelt es um bewährte und

effektive Maßnahmen, die derzeit auf dem Markt verfügbar sind; Konkretisierung bieten anerkannte nationale oder internationale Standards (z.B. von BSI, ENISA, NIST, TeleTrust).

2.1. Vertraulichkeit der Systeme und Dienste

Definition: Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen; vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

2.1.1. Physischer Schutz der Vertraulichkeit

Festlegung und Dokumentation zutrittsberechtigter Personen, einschließlich des Umfanges der Berechtigung	☒
Existenz von Zutrittsregeln-Regelungen für Firmenfremde	☒
Umsetzung einer Schlüsselregelung	☒
Ausgabe von Zutrittsberechtigungsausweisen	☒
Pforten- und Empfangspersonal während der Betriebszeiten	☒
Physische Schutzmaßnahmen sind vorhanden und werden regelmäßig überprüft:	
• gesicherter Eingang durch Ausweisleser	☒
• einbruchhemmende Fenster	☒
• Überwachungseinrichtung (z.B. Alarmanlage, Videoüberwachung)	☒
• Unterteilung in verschiedene Sicherheitszonen	☒
• Arbeitsplatzrechner sind in verschlossenen Räumen	☒
• Räume mit Servern sind alarmüberwacht	☒
• Maßnahmen gegen einfaches Mithören und Einsichtnahme	☒
• Ausdruck-Erstellung an definierte Gebäude-Zonen gebunden oder durch persönliches Drucken (z.B. Print-to-me, follow-me print, mit PIN)	☒
• Aktenvernichtung ausschließlich innerhalb definierter Zonen (z.B. durch Schredder)	☒
• Bewegungs-Sensoren, Glasbruch-Sensoren oder Bilderkennung	☒
• Unverzügliche Abarbeitung der Alarmmeldungen nach Alarmplan	☒

2.1.2. Schutz des Systemzugangs

Angemessener Passwortschutz (verbindliche dokumentierte Vorgaben)	☒
• (System-)Passwörter werden nicht im Klartext gespeichert	☒
• (System-)Passwörter werden nach dem Stand der Technik gehashed gespeichert	☒
Konzeption und Implementierung eines Berechtigungskonzepts	
• Berechtigungskonzept für Endgeräte (Rechner)	☒
• Berechtigungskonzept für IT-Applikationen/IT-Systemen	☒
Weitere Interaktionen mit dem IT-System sind nur nach einer erfolgreichen Authentifizierung möglich	☒
Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen und mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugriffsmöglichkeit aus dem Internet)	☒
Für die Administration des oder der IT-Systeme werden ausschließlich starke Passwörter mit mindestens 16 Zeichen verwendet	☒
Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)	☒
Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle	☒
Spezielle Sicherheitssoftware (z.B. Anti-Malware-SW, VPN, Firewall)	☒
Eine Segmentierung der genutzten Netze ist definiert	☒
Arbeitsplatzrechner sind in verschlossenen Räumen	☒
Aktenvernichter/-schredder (mind. Stufe 3, cross cuting)	☒

2.1.3. Berechtigungsmanagement

Anmerkung: Das Berechtigungsmanagement stützt auch das Schutzziel der Integrität

Die Verwendung von eindeutigen und personalisierten Benutzerkonten ist festgelegt	☒
Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer	☒
Berechtigungs- und Rollenkonzept für IT-Applikationen/IT-Systeme sind dokumentiert und umgesetzt	☒
Zugriffsberechtigungen und -beschränkungen gemäß „Need-to-Know“ und „Least Privilege“	☒
Regelmäßige Überprüfung der Berechtigungen	☒
Berechtigungsprüfung und Kontrolle der Zugangsbefugnisse aller Benutzer erfolgt auch innerhalb eines IT-Systems (z.B. Modul, Tabelle, Datensatz)	☒
Revisionssichere Dokumentation von Benutzerberechtigungen	☒

Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)	☒
Die Nutzung von "Sammel-Konten" ist geregelt (z. B. eingeschränkt, nur wenn auf den Nachweis der Handlungen verzichtet werden kann)	☒
Benutzerbezogene Zugänge zu Daten des Verantwortlichen dürfen nicht von mehreren Benutzern verwendet werden	☒
Ein Basis-Benutzerkonto mit minimalen Zugriffsrechten und Funktionalitäten ist vorhanden und wird angewendet	☒
Veränderungen der Zuständigkeiten von Mitarbeitern oder dem Arbeitsverhältnis mit diesen werden dem Systemadministrator umgehend mitgeteilt oder die Benutzerzugänge werden entsprechend angepasst	☒
Protokollierung von Events	
• Protokollierung des lesenden Zugriffs	☒
• Protokollierung des schreibenden Zugriffs (inkl. Löschung/Überschreiben)	☒
• Protokollierung von unberechtigten Zugriffsversuchen	☒
• Regelmäßige Auswertung	☒
• Anlassbezogene Auswertung	☒
Ein Management-Prozess (Vergabe/Änderung/Löschung) für privilegierte Benutzerkennungen ist dokumentiert und etabliert	☒
Die Vergabe von privilegierten Rechten erfolgt erst nach ausdrücklicher dokumentierter Genehmigung	☒
Es werden sichere Authentifizierungsverfahren für privilegierte Benutzerkonten verwendet	☒
Benutzerkonten mit privilegierten Rechten sind dokumentiert und werden regelmäßig überprüft	☒

2.1.4. Verschlüsselung

Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik	☒
Für die relevanten IT-Systeme ist die Verwaltung des Schlüsselmaterials definiert und dokumentiert	☒
Verschlüsselte Speicherung von personenbezogenen Daten	☒
Ein Regelwerk mit Anforderungen an die Verschlüsselungsstärke, die Verwaltung der Schlüssel, dem Verschlüsselungsalgorithmus ist dokumentiert und umgesetzt	☒

2.1.5. Pseudonymisierung

Pseudonymisieren durch Einwegfunktionen	☒
Pseudonymisieren durch Zuordnungstabellen:	
• Zugriffe werde differenziert nach Lesen, Schreiben, Löschen (auf dem IT-System, das die Zuordnungstabellen verwaltet) in Protokollen dokumentiert	☒
• Zuordnungstabellen sind organisatorisch von Kernbetrieb der in Rede stehenden Datenverarbeitung getrennt	☒

2.2. Integrität der Systeme und Dienste

Definition: Eine unerlaubte oder unbeabsichtigte Veränderung stellt eine Verletzung der Integrität von Informationen dar; dies kann neben dem eigentlichen Inhalt auch Attribute wie den Urheber oder Absender sowie den Zeitpunkt der Erstellung betreffen. Integrität kann sich sowohl auf die Unversehrtheit von Daten als auch auf die korrekte Funktionsweise von Systemen beziehen.

2.2.1. Schutz der Datenübertragung

Anmerkung: Der Schutz der Datenübertragung stützt auch das Schutzziel der Vertraulichkeit.

Vollständige Dokumentation der Wege der Weitergabe von personenbezogenen Daten im Zuge dieser Auftragsverarbeitung (z.B. Ausdruck, Datenträger, automatisierte Übermittlung, WAN-Strecke, TLS)	☒
Definition und Dokumentation der Empfänger von personenbezogenen Daten im Kontext der hier vereinbarten Auftragsverarbeitung	☒
Sicherungen des Transports (z.B. sicheres Fahrzeug, Behälter, Verschlüsselung von Speichermedien, Übergabeprotokolle, TLS-verschlüsselte Übermittlung)	☒
Dokumentationen aller Schnittstellen und der Abruf- und Übermittlungsprogramme	☒
Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen:	
• Deaktivierung von USB-Schnittstellen	☒
• Beschränkung der Befugnisse zur Datenübertragung	☒
• Regelmäßige Kontrolle der zulässigen Empfänger	☒
• Technische Beschränkung auf zulässige Empfänger	☒
• Data Loss Prevention Lösungen werden eingesetzt	☒
Durchführung von Protokollierungen einer elektronischen Datenweitergabe oder Übermittlung	☒

2.2.2. Eingabkontrolle

Protokollierung der Eingaben von und Änderungen an personenbezogenen Daten	☒
Regelmäßige Überprüfung der Protokolle zu Eingaben/Änderungen personenbezogener Daten	☒
Organisatorisch festgelegt Zuständigkeiten für die Eingabe	☒

2.2.3. Weitere Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste

Das Minimalprinzip wird eingehalten (z. B. Einschränkung der Berechtigungen, Ports, Protokolle, Software)	☒
Es erfolgt eine automatische Überprüfung der von zentralen Gateways transportierten Daten (z.B. E-Mail, Internet, Netze von Dritten) mittels einer Schutzsoftware (inkl. verschlüsselter Verbindungen)	☒
Mandantenfähigkeit:	
• Dedizierte physische Server	☒
• Trennung auf Systemebene	☒
• Trennung auf Datenebene	☒
Beschreibung der Umsetzung der Mandantentrennung	
• Es ist sichergestellt, dass durch eine wirksame Trennung unbefugte Nutzer von Organisationen nicht auf personenbezogene Daten anderer Organisationen zugreifen können	☒
• Gemeinsam genutzte virtuelle Maschinen und/oder Applikationsinstanzen sind entsprechend gehärtet	☒
• Eine Separierung von Daten, Applikationen, Betriebssystem, Storage und Netzwerk ist umgesetzt	☒
• Dedizierte physische Leitungen zur Datenübertragung	☒
Es erfolgt eine automatische Überprüfung von empfangenen Dateien und Programmen vor deren Ausführung auf Schadsoftware (On-Access-Scan)	☒
Es erfolgt eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware	☒
Es existiert ein Intrusion Detection System	☒
Zweckattribute sind für Datenfelder und –sätze definiert und umgesetzt worden	☒

2.3. Verfügbarkeit der Systeme und Dienste

Definition: Verfügbarkeit von [Daten,] Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen bedeutet, dass diese von den Anwendern stets wie vorgesehen genutzt werden können.

2.3.1. Sicherung der Verfügbarkeit personenbezogener Daten

Anmerkung: Die Sicherung der Verfügbarkeit personenbezogener Daten stützt auch das Schutzziel der Integrität.

Vorhandensein von redundanten IT-Systemen (Endgeräte, Server, Speicher etc.)	☒
Unterbrechungsfreie Stromversorgung (USV)	☒
Funktionsfähige physische Schutzeinrichtungen für Brandschutz, Energieversorgung, Klimatisierung)	☒
Serverräume und Rechenzentren verfügen über Feuer- und Rauchmeldeanlagen	☒
Serverräume und Rechenzentren verfügen über Feuerlöscher bzw. Feuerlöschanlagen	☒
Serverräume und Rechenzentren verfügen über Anlagen zur Überwachung von Temperatur und Feuchtigkeit	☒
Regelmäßige Kontrollen des Systemzustandes (Monitoring)	☒
Vorhandensein von divers ausgelegten IT-Systemen (gleiche Funktionalität von unterschiedlichen Herstellern)	☒

2.3.2. Löschung

Definition: Das Ergebnis der Löschung ist die (faktische) Unmöglichkeit die zuvor in den Daten verkörperte Information wahrzunehmen..

Definition und Dokumentation von Löschfristen für Daten (Löschkonzept)	☒
Umsetzung der Löschung gemäß der Löschfristen für Daten	☒
Definition und Dokumentation von Verfahren zur Entsorgung und Vernichtung von Datenträgen	☒
Umsetzung von Regelungen zum Umgang mit elektr. Speichermedien	☒
Umsetzung von Regelungen zur Entsorgung von Speichermedien	☒
Integritätskontrolle bei Löschungen bzw. Löschroutinen	☒
Umgesetzte Löschung auf Entwicklungs-, Test- und Produktivumgebungen	☒

2.4. Belastbarkeit der Systeme und Dienste

Definition: Belastbarkeit der Systeme u. Dienste beschreibt die Absicherung der Werte (hier: personenbezogene Daten) gegen ungewollten, zufälligen oder unrechtmäßigen Verlust oder Einschränkung (Störungen) von einem oder mehreren der klassischen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) sowie, dass Systeme und Dienste nach einer Störung in angemessener Zeit wieder in den Normalbetrieb überführt werden können. Im Falle einer Störung sollen deren Auswirkungen auf die drei vorherig beschriebenen klassischen Schutzziele möglichst gering sein.

2.4.1. Absicherung gegen Störungen (Kontinuitätssicherung)

Anmerkung: Die Sicherung der Verfügbarkeit personenbezogener Daten stützt auch das Schutzziel der Integrität.

Virenscanner mit aktuellen Suchmustern	☒
Redundant ausgelegte IT-Systeme	☒
Maßnahmen zur Steigerung der Aufrechterhaltung der Funktionalität von Systemen	☒
Moderne Firewall Systeme	☒
Ein RAID-System wird betrieben	☒
Intrusion Detection Systeme	☒
Maßnahmen zur Steigerung der Fehlertoleranz von Systemen und Diensten	☒
Unverzügliche Wiederherstellung der Verfügbarkeit	☒
Bei Websites und Webanwendungen: Content-Security-Policy (CSP) ist definiert und umgesetzt	☒

2.4.2. Wiederanlauf und Wiederherstellung der Verfügbarkeit

Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen)	☒
Dokumentiertes und getestetes Notfallkonzept	☒

2.5. Organisatorische und prozessual Schutzmaßnahmen

Durch organisatorische und prozessuale Schutzmaßnahmen werden die oben genannten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit nachhaltig abgesichert.

2.5.1. Organisatorische Sicherheitsmaßnahmen

Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz	☐
Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit	☒
Existenz eines angemessenen Informationssicherheitsmanagements	☒
Existenz eines angemessenen Incident Managements (Reaktion auf Sicherheitsverletzungen)	☒
Es existiert eine Angriffserkennung und Meldungsmöglichkeiten (Incident-Responce)	☒
Schriftlich dokumentierter Change Management Prozess für IT-Systeme die personenbezogene Daten im Kontext diese Vertrages verarbeiten	☒
Schriftlich dokumentierter und getesteter Patch Management Prozess für IT-Systeme die personenbezogene Daten im Kontext diese Vertrages verarbeiten	☒
Informationen über technische Schwachstellen zu den genutzten Assets werden gesammelt und bewertet	☒
Vorlage eines Sicherheitskonzepts nach behördlichen Mindestanforderungen (z.B. BSI)	☒
Potenziell von technischen Schwachstellen betroffene Systemen und Software (Assets) werden identifiziert (z. B. Hersteller, Version, Installationsort)	☒
Gewährleistung von Reaktionsmöglichkeiten bei technischen Schwachstellen:	
• Abtrennung der betroffenen Systeme	☒
• Abschalten des betroffenen Service	☒
• Anpassung von Zugriffsmöglichkeiten wie z. B. Firewalls	☒
• Anpassen des Monitorings	☒
• Erhöhung der Awareness der Anwender	☒
Durchführung einer Informationsklassifizierung	☒
In der Test- und Entwicklungsumgebung werden nur synthetische Daten, also keine Echtdaten oder personenbezogene Daten verarbeitet	☒
Die Nutzung von mobilen Endgeräten (z. B. Smartphones, Notebooks) durch Mitarbeiter außerhalb der Liegenschaften und Büros ist geregelt	☒

Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme	☒
Prozess zur regelmäßigen Überprüfung der Wirksamkeit aller Schutzmaßnahmen und gegebenenfalls deren Anpassung zur Gewährleistung der Sicherheit der Verarbeitung	☒

2.5.2. Auftragskontrolle

Dokumentation aller Subunternehmer, die für die Verarbeitung der in diesem Vertrag beschriebenen personenbezogenen Daten eingesetzt werden	☒
Es erfolgen regelmäßige Subunternehmer-Audits	☒
Dokumentierte Prozesse der gesamten Organisation liegen vor	☒
Es liegen historisierte und versionisierte SLAs und OLAs vor	☒
Es existiert ein vollständiges Qualitäts-Management System bei den relevanten Subunternehmern	☒
Es existiert ein vollständiges Informationssicherheits-Management System (ISMS)bei den relevanten Subunternehmern	☒
Alle eingesetzten den relevanten Subunternehmern verfügen über eine Zertifizierung in BereichInformationssicherheit, ausgestellt von einer akkreditierten Zertifizierungsstelle(z.B. ISO 27001, TISAX, SOC 2, BSI IT-Grundschutz)	☒
Die regelmäßige Kontrolle der relevanten Subunternehmer erfolgt durch	
• Vorlage von Self-Assessments	☒
• Vorlage der Verträge mit (weiteren) Subunternehmern	☒
• Durchführung von Kontrollen bei Subunternehmern	☒
Vorhandensein von Richtlinien und Arbeitsanweisungen für die Verarbeitung im Auftrag	☒

ANHANG I: GENEHMIGTE SUBUNTERNEHMER

Auftragsverarbeiter	Anschrift	Teilleistung
EIKONA AG	Am Alten Bahnhof 8, D-97332 Volkach, Deutschland	Erbringung von Dienstleistungen rund um Finanzbuchhaltung, Rechnungslegung, Mahnwesen und Personalverwaltung
EIKONA Systems GmbH	Am Alten Bahnhof 8, D-97332 Volkach, Deutschland	Administrative Betreuung der IT-Infrastruktur, 1st und 2nd Level Support für Fleetboard Personal und Mitarbeiter des Auftraggebers, Consulting im Zusammenhang mit Datenschutz und IT-Sicherheitsmaßnahmen
Atlassian B.V.	c/o Atlassian Inc., 350 Bush Street, San Francisco, CA 94104	3rd Level-Support im Zusammenhang mit dem eingesetzten Collaborationstools (JIRA, Confluence)
Reddoxx GmbH	Neue Weilheimer Straße 14, D-73230 Kirchheim	3rd Level Support im Rahmen der eingesetzten SPAM-Filter und revisionssicheren Mailarchi-vierungslösung der Fleetboard Logistics GmbH
Sage GmbH	Franklinstraße 61-63, D-60486 Frankfurt/Main	3rd Level Support im Rahmen der eingesetzten Finanzbuchhaltungs- und Kundenverwaltungssoftware
Swyx Solutions GmbH	Emil-Figge-Straße 86, D-44227 Dortmund	3rd Level-Support im Rahmen der eingesetzten Telefonserver-Software der Fleetboard Logistics GmbH
GRAFINIT Korlatolt Felelössegü Tarsasag	1114 Budapest, Bartok Bela ut 15/d II em. Ungarn	Entwicklerteam, Unterstützung bei der Programmierung von einzelnen Komponenten der conizi-Plattform und angeschlossener Micro-Services
LUNISA trust & match GmbH	Am Alten Bahnhof 8, D-97332 Volkach	Erbringung von Personaldienstleistungen im Rahmen von Bewerbungsprozessen und Mitarbeitermaßnahmen
DeepL GmbH	Maarweg 165, D-50825 Köln	Zur Verfügung stellen der Übersetzungsfunktion im Chat für die HABBL App mithilfe einer API-Schnittstelle.

Der Auftragsverarbeiter versichert, dass die hier aufgeführten Subunternehmer vertraglich an die Verpflichtungen des Teils 1 gebunden sind und die technischen und organisatorischen Maßnahmen gemäß den Festlegungen des Teils 2 implementiert haben.