Vereinbarung zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO

Stand: 01. Oktober 2025

Zwischen

dem Kunden der Fizard GmbH

(nachfolgend „**Auftraggeber**“ oder „**Verantwortlicher**“)

und

der Fizard GmbH, St.-Cajetan-Str. 5, 81669 München

(nachfolgend „**Auftragnehmer**“ oder „**Fizard**“)

Präambel

Diese Vereinbarung zur Auftragsverarbeitung (AVV) konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Nutzung der Software-as-a-Service (SaaS) Lösung „Fizard“ durch den Auftraggeber. Grundlage dieser AVV ist der zwischen den Parteien geschlossene Vertrag (nachfolgend „Hauptvertrag“, insbesondere die AGB).

Im Falle von Widersprüchen haben die Regelungen dieser AVV Vorrang vor den Regelungen des Hauptvertrages, soweit sie datenschutzrechtliche Aspekte betreffen.

§ 1 Definitionen

Soweit in dieser AVV nicht abweichend definiert, entsprechen die verwendeten Begriffe den Definitionen der EU-Datenschutz-Grundverordnung (DSGVO). Es gelten insbesondere folgende Definitionen:

(1) Personenbezogene Daten, Verarbeitung, Verantwortlicher, Auftragsverarbeiter entsprechen den Definitionen in Art. 4 DSGVO.

(2) Technische und Organisatorische Maßnahmen (TOMs) sind die Maßnahmen gemäß Art. 32 DSGVO.

(3) Unterauftragsverarbeiter (Subunternehmer) sind vom Auftragnehmer eingesetzte Dritte, die personenbezogene Daten für den Auftragnehmer im Auftrag des Verantwortlichen verarbeiten. Nicht als Unterauftragsverarbeitung im Sinne dieser AVV gelten Nebenleistungen, die bei

Dritten in Anspruch genommen werden (z.B. Transport, Postversand, Reinigung, Telekommunikationsdienstleistungen ohne konkreten Bezug zu Leistungen für den Auftraggeber).

(4) Drittland ist jedes Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR).

§ 2 Gegenstand, Dauer, Art und Zweck der Verarbeitung

(1) **Gegenstand und Dauer**: Gegenstand dieser AVV ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer zur Erbringung der im Hauptvertrag vereinbarten Leistungen. Die Dauer richtet sich nach der Laufzeit des Hauptvertrages.

(2) **Art der Verarbeitung (Leistungsbeschreibung)**: Die Verarbeitung umfasst insbesondere:

a) Automatisierter Abruf von Transaktionsdaten aus dem Stripe-Konto des Auftraggebers.
b) Speicherung und Hosting dieser Daten.
c) Verarbeitung (Aufbereitung, Validierung, Zuordnung) gemäß den Konfigurationen des Auftraggebers.
d) Konvertierung in DATEV-kompatible Formate und Bereitstellung zum Export.
e) Löschung der Daten gemäß vertraglichen Vorgaben.

Es findet keine automatisierte Entscheidungsfindung im Einzelfall gemäß Art. 22 DSGVO durch den Auftragnehmer statt.

(3) **Ort der Verarbeitung (Hosting-Standort)**: Die primäre Speicherung und Verarbeitung der Produktivdaten erfolgt standardmäßig in Rechenzentren innerhalb der EU/des EWR. Eine Verarbeitung in einem Drittland (außerhalb der EU/EWR) erfolgt nur im Rahmen des Einsatzes von Unterauftragsverarbeitern (z.B. für Monitoring, Support-Zugriffe oder global erbrachte Dienste) und ausschließlich auf Basis eines gültigen Transfermechanismus gemäß Kap. V DSGVO (Details in § 7 und Anlage 2).

(4) **Zweck der Verarbeitung**: Die Verarbeitung dient ausschließlich der Automatisierung der vorbereitenden Finanzbuchhaltung für den Auftraggeber. Eine Verarbeitung für eigene Zwecke des Auftragnehmers ist untersagt, es sei denn, es handelt sich um vollständig und irreversibel anonymisierte Daten gemäß Hauptvertrag oder der Auftragnehmer ist gesetzlich dazu verpflichtet.

§ 3 Kategorien betroffener Personen und Arten personenbezogener Daten

(1) **Kategorien betroffener Personen**:

a) Endkunden des Auftraggebers (Zahler, Rechnungsempfänger in Stripe).
b) Mitarbeiter, Ansprechpartner und autorisierte Nutzer des Auftraggebers.
c) Ggf. Lieferanten oder Geschäftspartner des Auftraggebers, soweit deren Daten in den Stripe-Transaktionen enthalten sind.

(2) **Arten personenbezogener Daten**:

a) Stammdaten (Name, Firma, Anschrift, E-Mail, Steuernummern).
b) Vertrags- und Abrechnungsdaten (Beträge, Steuersätze, Rechnungsnummern).
c) Belegdaten (z.B. Rechnungsdokumente/PDFs).
d) Zahlungsdaten (Status, Art, Zeitpunkt, Transaktions-IDs).
e) Nutzungsdaten der Fizard-Nutzer (IP-Adressen, Login-Zeiten, Audit-Logs).

(3) **Besondere Kategorien personenbezogener Daten**: Es werden wissentlich keine Daten gemäß Art. 9 oder Art. 10 DSGVO verarbeitet. Der Auftraggeber stellt sicher, dass in frei gestaltbaren Feldern (z.B. Freitextfelder, Notizen) keine solchen Daten verarbeitet werden.

§ 4 Pflichten und Weisungsbefugnis des Auftraggebers (Verantwortlicher)

(1) **Verantwortlichkeit**: Der Auftraggeber ist allein verantwortlich für die datenschutzrechtliche Zulässigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen (Art. 12 ff. DSGVO). Ihm obliegen die Informationspflichten (Art. 13, 14 DSGVO).

(2) **Weisungsrecht und Konfiguration**: Der Auftraggeber hat das umfassende Recht zur Erteilung dokumentierter Weisungen. Der Hauptvertrag, diese AVV sowie die Konfiguration und Nutzung der Software durch den Auftraggeber gelten als dokumentierte Weisungen.

(3) **Form und Mehraufwand**: Einzelweisungen sind in Textform zu erteilen. Führen Einzelweisungen zu einem Mehraufwand, der über die vereinbarten Leistungen hinausgeht, ist dieser vom Auftraggeber nach vorheriger Ankündigung durch den Auftragnehmer angemessen zu vergüten.

(4) **Kontrollrechte**: Der Auftraggeber hat das Recht zur Kontrolle der Einhaltung dieser AVV und der TOMs (Details in § 9).

§ 5 Pflichten des Auftragnehmers (Auftragsverarbeiter)

(1) **Weisungsgebundene Verarbeitung**: Der Auftragnehmer verarbeitet Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist gesetzlich zu einer anderen Verarbeitung verpflichtet. In diesem Fall informiert er den Auftraggeber vorab, sofern zulässig.

(2) **Warnpflicht**: Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Datenschutzvorschriften verstößt. Er ist berechtigt, die Durchführung der betreffenden Weisung bis zur Klärung oder Bestätigung durch den Auftraggeber auszusetzen.

(3) **Vertraulichkeit**: Der Auftragnehmer gewährleistet, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden (Art. 28 Abs. 3 lit. b DSGVO).

(4) **Sicherheit (TOMs)**: Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen (Details in § 6 und Anlage 1).

(5) **Unterstützungspflichten**: Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrung der Betroffenenrechte (Details in § 8) sowie bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldungen, Datenschutz-Folgenabschätzungen (DSFA)). Für Unterstützungsleistungen, die nicht auf einem Verschulden des Auftragnehmers beruhen und über den vereinbarten Leistungsumfang hinausgehen, kann der Auftragnehmer nach vorheriger Ankündigung eine angemessene Vergütung verlangen.

(6) **Rückgabe und Löschung**: Nach Abschluss der Leistungen löscht oder gibt der Auftragnehmer die Daten zurück (Details in § 11).

(7) **Verarbeitungsverzeichnis**: Der Auftragnehmer führt ein Verzeichnis gemäß Art. 30 Abs. 2 DSGVO.

(8) **Umgang mit Behördenanfragen**: Der Auftragnehmer informiert den Auftraggeber unverzüglich über behördliche Auskunfts- oder Zugriffsersuchen in Bezug auf die Auftragsdaten, soweit rechtlich zulässig. Er wird den Auftraggeber bei der Beantwortung und, soweit erforderlich und zumutbar, bei der Abwehr solcher Ersuchen unterstützen. Direkte Auskünfte an Behörden erteilt der Auftragnehmer nur, wenn er hierzu gesetzlich verpflichtet ist.

§ 6 Technische und Organisatorische Maßnahmen (TOMs)

(1) **Verpflichtung auf Sicherheit**: Der Auftragnehmer verpflichtet sich, geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) **Konkrete Maßnahmen (Anlage 1)**: Die implementierten TOMs sind in der Anlage 1 beschrieben. Der Auftraggeber hat diese TOMs geprüft und erkennt sie auf dieser Grundlage als ausreichend an.

(3) **Anpassung und Überprüfung**: Der Auftragnehmer überprüft die Wirksamkeit der TOMs regelmäßig und passt sie fortlaufend an den Stand der Technik an. Der Auftragnehmer darf die TOMs weiterentwickeln oder durch gleichwertige Maßnahmen ersetzen, sofern das vereinbarte

Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dem Auftraggeber vorab mit angemessener Frist (in der Regel 30 Tage) angekündigt.

§ 7 Einsatz von Unterauftragsverarbeitern (Subunternehmern)

(1) **Allgemeine Genehmigung**: Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung gemäß Art. 28 Abs. 2 DSGVO, Unterauftragsverarbeiter hinzuzuziehen.

(2) **Bestehende Unterauftragsverarbeiter und Liste**: Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in der Anlage 2 aufgeführt und gelten als genehmigt. Der Auftragnehmer führt eine öffentlich zugängliche Liste der Unterauftragsverarbeiter und bietet eine Möglichkeit zur Benachrichtigung über Änderungen (z.B. per E-Mail-Abonnement).

(3) **Informationspflicht bei Änderungen**: Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) in Textform (z.B. über die Benachrichtigungsfunktion gemäß Abs. 2). Die Information erfolgt mit einer angemessenen Frist, in der Regel 30 Tage vor dem Einsatz. Bei dringenden Sicherheits- oder Betriebserfordernissen kann die Frist angemessen verkürzt werden; der Auftraggeber wird in diesem Fall unverzüglich informiert.

(4) **Widerspruchsrecht**: Der Auftraggeber kann gegen die Änderung innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund Widerspruch einlegen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

(5) **Folgen des Widerspruchs**: Legt der Auftraggeber begründeten Widerspruch ein und kann keine einvernehmliche Lösung gefunden werden, steht beiden Parteien ein Sonderkündigungsrecht zu. Der Auftraggeber ist zur Kündigung der betroffenen Leistungen oder des Hauptvertrags berechtigt. Der Auftragnehmer ist zur Kündigung des Hauptvertrags mit einer Frist von einem Monat berechtigt, sofern die Leistungserbringung ohne den Unterauftragsverarbeiter für ihn unzumutbar wäre.

(6) **Vertragliche Verpflichtungen (Flow-Down) und Haftung**: Der Auftragnehmer stellt sicher, dass dem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegt werden wie in dieser AVV. Der Auftragnehmer bleibt gegenüber dem Auftraggeber voll verantwortlich.

(7) **Verarbeitung in Drittländern (Drittlandtransfer)**: Eine Übermittlung von Daten in Drittländer erfolgt ausschließlich auf Basis eines gültigen Transfermechanismus nach Kap. V DSGVO. Es gelten folgende Mechanismen (Details in Anlage 2):

a) **Angemessenheitsbeschluss (Art. 45 DSGVO)**: Übermittlungen in Länder mit gültigem Angemessenheitsbeschluss erfolgen auf dieser Grundlage. Dies gilt insbesondere für Übermittlungen in die USA an Empfänger, die unter dem EU-US Data Privacy Framework (DPF) zertifiziert sind.

b) **Standarddatenschutzklauseln (SCCs, Art. 46 Abs. 2 lit. c DSGVO)**: Liegt kein Angemessenheitsbeschluss vor oder deckt dieser die Übermittlung nicht ab, erfolgt sie auf Basis von EU-SCCs. In diesem Fall stellt der Auftragnehmer sicher, dass durch eine dokumentierte Risikoanalyse (Transfer Impact Assessment, TIA) und ggf. erforderliche zusätzliche Maßnahmen (z.B. Verschlüsselung, Pseudonymisierung) ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet ist.

Informationen hierzu sind in Anlage 2 aufgeführt.

§ 8 Rechte der betroffenen Personen

(1) **Verantwortung**: Die Verantwortung für die Bearbeitung von Anfragen betroffener Personen (Art. 15-22 DSGVO) liegt beim Auftraggeber.

(2) **Unterstützungspflicht**: Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen.

(3) **Umfang**: Der Auftragnehmer ermöglicht dem Auftraggeber vorrangig, Anfragen durch Funktionen der Software selbst zu bearbeiten (Self-Service). Soweit dies nicht möglich ist, wird der Auftragnehmer auf dokumentierte Weisung tätig. Die Unterstützung erfolgt unverzüglich, spätestens innerhalb von 5 Geschäftstagen nach Anforderung.

(4) **Direkte Anfragen**: Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

(5) **Vergütung**: Für Unterstützungsleistungen, die nicht durch einen Fehler des Auftragnehmers verursacht wurden und über den vereinbarten Leistungsumfang hinausgehen, kann der Auftragnehmer nach vorheriger Ankündigung eine angemessene Vergütung verlangen.

§ 9 Kontrollrechte des Auftraggebers (Audits)

(1) **Nachweispflicht**: Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung dieser AVV zur Verfügung.

(2) **Standardnachweise (Dokumentation/Remote-Audits)**: Der Nachweis erfolgt vorrangig durch die Bereitstellung aktueller Dokumentationen (z.B. Selbstauskünfte, Zertifikate wie ISO 27001, SOC 2) oder durch Remote-Audits. Der Auftragnehmer stellt auf Anforderung eine Zusammenfassung (Executive Summary) von externen Penetrationstest-Berichten bereit.

(3) **Überprüfungen (Vor-Ort-Audits)**: Sofern die Standardnachweise im Einzelfall begründet nicht ausreichen oder ein begründeter Anlass besteht (z.B. wesentlicher Sicherheitsvorfall), ist der Auftraggeber berechtigt, selbst oder durch einen zur Verschwiegenheit verpflichteten,

sachkundigen Dritten Inspektionen vor Ort durchzuführen. Der Dritte darf nicht im Wettbewerb zum Auftragnehmer stehen und muss seine Qualifikation auf Verlangen nachweisen.

(4) **Durchführung von Vor-Ort-Audits**: Inspektionen vor Ort finden nach Anmeldung mit angemessener Frist (in der Regel vier Wochen) statt. Die Häufigkeit ist grundsätzlich auf ein Mal pro Kalenderjahr begrenzt.

(5) **Vertraulichkeit und Kosten**: Der Auftraggeber behandelt alle erlangten Informationen vertraulich. Er trägt die ihm entstehenden Kosten. Der Auftragnehmer kann für seinen Unterstützungsaufwand eine angemessene Vergütung verlangen, es sei denn, das Audit deckt erhebliche Verstöße des Auftragnehmers auf, die dieser zu vertreten hat.

§ 10 Meldepflichten bei Datenschutzverletzungen

(1) **Meldepflicht des Auftragnehmers**: Der Auftragnehmer meldet dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten (Datenschutzverletzung) ohne unangemessene Verzögerung. Die Erstmeldung erfolgt möglichst binnen 24 Stunden nach Kenntniserlangung an die vom Auftraggeber hinterlegte Kontaktadresse.

(2) **Inhalt der Meldung**: Die Meldung muss mindestens die verfügbaren Informationen gemäß Art. 33 Abs. 3 DSGVO enthalten.

(3) **Sukzessive Meldung**: Wenn Informationen nicht gleichzeitig bereitgestellt werden können, stellt der Auftragnehmer sie ohne unangemessene weitere Verzögerung schrittweise bereit (rollierende Meldung), bis ein Abschlussbericht vorliegt.

(4) **Maßnahmen und Unterstützung**: Der Auftragnehmer ergreift unverzüglich erforderliche Maßnahmen und unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten gemäß Art. 33 und 34 DSGVO.

§ 11 Rückgabe und Löschung der Daten nach Vertragsende

(1) **Wahlrecht**: Nach Beendigung des Hauptvertrages ist der Auftragnehmer gemäß Art. 28 Abs. 3 lit. g DSGVO verpflichtet, sämtliche im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers zurückzugeben oder zu löschen, sofern keine gesetzliche Speicherpflicht besteht.

(2) **Prozess zur Rückgabe (Export)**: Die Rückgabe erfolgt durch die Möglichkeit des Auftraggebers, die Daten innerhalb der im Hauptvertrag vereinbarten Zugriffsphase (Grace Period) selbstständig zu exportieren.

(3) **Löschungsprozess**: Der Auftragnehmer wird die im Auftrag verarbeiteten Daten nach Ablauf der Zugriffsphase unwiederbringlich aus den Produktivsystemen löschen.

(4) **Löschung von Backups**: In Backups enthaltene Daten werden im Rahmen des regulären Backup-Rotationszyklus endgültig überschrieben. Bis dahin sind sie gesperrt (logisch getrennt) und vor unberechtigtem Zugriff geschützt.

(5) **Bestätigung**: Auf Anforderung bestätigt der Auftragnehmer die datenschutzkonforme Löschung in Textform.

(6) **Ausnahmen**: Gesetzliche Aufbewahrungspflichten des Auftragnehmers betreffen allein eigene Geschäftsunterlagen und nicht die im Auftrag verarbeiteten Kundendaten. Konfigurationsdaten ohne Personenbezug und Stammdaten des Kundenkontos bleiben gemäß Hauptvertrag gespeichert, bis der Auftraggeber deren Löschung verlangt.

§ 12 Haftung

(1) **Haftung im Innenverhältnis**: Für die Haftung der Parteien im Innenverhältnis gelten die Haftungsregelungen des Hauptvertrages.

(2) **Haftung gegenüber Betroffenen (Art. 82 DSGVO)**: Die gesetzliche Haftung der Parteien gegenüber betroffenen Personen gemäß Art. 82 DSGVO bleibt unberührt (Gesamtschuldnerhaftung).

(3) **Haftungsausgleich im Innenverhältnis**: Wird eine Partei für einen Schaden oder ein Bußgeld in Anspruch genommen, hat sie gegen die andere Partei einen Ausgleichsanspruch im Innenverhältnis entsprechend dem jeweiligen Anteil an der Verantwortung (Art. 82 Abs. 5 DSGVO).

§ 13 Schlussbestimmungen

(1) **Rangfolge**: Im Falle von Widersprüchen gehen die Regelungen dieser AVV in Bezug auf den Datenschutz dem Hauptvertrag vor.

(2) **Recht und Gerichtsstand**: Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand ist München, sofern der Auftraggeber Kaufmann ist.

(3) **Form**: Änderungen dieser AVV bedürfen der Textform oder können durch eine ausdrücklich vereinbarte und dokumentierte elektronische Form (z.B. Akzeptanz im Kundenkonto) erfolgen.

(4) **Salvatorische Klausel**: Sollten einzelne Bestimmungen unwirksam sein, wird die Wirksamkeit der übrigen Bestimmungen nicht berührt.

Anlage 1 zur AVV: Technische und Organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO

1. Einleitung

Diese Anlage beschreibt die vom Auftragnehmer (Fizard GmbH) getroffenen TOMs nach dem Stand der Technik. Die Maßnahmen basieren auf einer regelmäßigen Risikoanalyse, die die Sensibilität von Finanzdaten berücksichtigt und orientieren sich an anerkannten Standards (z.B. ISO 27001, BSI-Standards).

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

2.1. Zutrittskontrolle (Physische Sicherheit)

- **Cloud-Infrastruktur (Shared Responsibility)**: Die physische Sicherheit wird durch zertifizierte Infrastrukturanbieter (u.a. ISO 27001, SOC 2) gewährleistet. Die Maßnahmen umfassen angemessene physische Sicherheitsvorkehrungen (z.B. mehrstufige Sicherheitszonen, Zugangskontrollen, Überwachung).
- **Geschäftsräume und Remote Work**: Eigene Standorte sowie Remote-Arbeitsplätze sind durch organisatorische und technische Maßnahmen angemessen gesichert (z.B. Zutrittskontrollen, Verpflichtung zum Sperren von Endgeräten, Clean Desk Policy). Es wird keine kritische Infrastruktur vor Ort betrieben.

2.2. Zugangskontrolle (Systemzugang)

- **Authentifizierung**: Zugang erfordert eindeutige Benutzerkennung. Es gelten sichere Passwortrichtlinien nach dem Stand der Technik, deren Einhaltung technisch unterstützt wird (z.B. durch Passwort-Manager).
- **Multi-Faktor-Authentifizierung (MFA)**: MFA wird für administrative, privilegierte und Remote-Zugriffe sowie den Zugang zu kritischen Systemen eingesetzt.
- **Zentrale Verwaltung**: Die Verwaltung der Zugänge erfolgt zentralisiert.
- **Endgerätesicherheit (Endpoints)**: Es wird durch Richtlinien und technische Kontrollen sichergestellt, dass:
  - Festplattenverschlüsselung aktiviert ist.
  - Systeme aktuell gehalten werden (Patch-Management).
  - Bildschirme bei Inaktivität automatisch gesperrt werden.
- **Sperrung von Zugängen**: Dokumentierter Offboarding-Prozess zur sofortigen Sperrung aller Zugänge.

2.3. Zugriffskontrolle (Datenzugriff)

- **Berechtigungskonzept (Least Privilege & Need-to-Know)**: Einsatz von rollenbasierten Berechtigungskonzepten (RBAC). Vergabe nach dem Prinzip der minimalen Rechtevergabe.
- **Just-in-Time (JIT) Access und Segregation of Duties (SoD)**: Wo möglich, erfolgt die Vergabe von administrativen Rechten temporär und anlassbezogen (JIT). Funktionstrennung (SoD) und das Vier-Augen-Prinzip werden angewendet.
- **Zugriff auf Produktivdaten**: Direkter Zugriff auf Produktivdatenbanken erfolgt nur in dokumentierten Ausnahmefällen (z.B. Support auf Anforderung), wird streng protokolliert und erfordert gesonderte Freigabe (Break-Glass-Prozess).
- **Regelmäßige Überprüfung**: Regelmäßige Rezertifizierung der vergebenen Berechtigungen.

2.4. Trennungskontrolle

- **Mandantenfähigkeit**: Logische Trennung der Daten verschiedener Auftraggeber auf Anwendungsebene.
- **Trennung von Umgebungen**: Strikte Trennung von Entwicklungs-, Test- und Produktivumgebungen. In Testumgebungen werden grundsätzlich nur synthetische, pseudonymisierte oder anonymisierte Daten verwendet.

2.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

- Personenbezogene Daten werden in internen Logs und bei der Fehleranalyse nach Möglichkeit und Zweckmäßigkeit pseudonymisiert oder gefiltert (PII-Redaction).

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

3.1. Weitergabekontrolle (Verschlüsselung)

- **Verschlüsselung in Transit**: Datenübertragungen erfolgen über sichere Verbindungen nach dem Stand der Technik (z.B. aktuelle TLS-Profile).
- **Verschlüsselung at Rest**: Daten in Datenbanken, Objektspeichern und Backups werden im Ruhezustand unter Einsatz starker Verschlüsselungsverfahren nach dem Stand der Technik verschlüsselt.
- **Schlüssel- und Secrets-Management**: Es wird ein sicheres Schlüsselmanagement angewendet. Nutzung von sicheren Mechanismen zur Verwaltung von Schlüsseln und Zugangsdaten. Es bestehen Prozesse zur Rotation von Schlüsseln bei Bedarf oder Kompromittierung.
- **Sicherer Remote-Zugriff**: Der administrative Zugriff erfolgt ausschließlich über verschlüsselte Protokolle und starke Authentifizierung.

- **Content Delivery Networks (CDNs)**: Konfigurationen (z.B. Cache-Control-Header) stellen sicher, dass keine Zwischenspeicherung personenbezogener Inhalte erfolgt oder diese angemessen abgesichert ist.

3.2. Eingabekontrolle (Protokollierung)

- **Anwendungsprotokollierung (Audit Logs)**: Protokollierung von wesentlichen Aktionen innerhalb der Anwendung und Änderungen an der Infrastruktur zur Nachvollziehbarkeit.
- **Logging & Monitoring Systeme**: Einsatz spezialisierter Dienste. Maßnahmen zur PII-Minimierung in Logs sind implementiert.
- **Log-Retention**: Protokolle sind angemessen vor Manipulation geschützt. Die Aufbewahrung erfolgt zweck- und risikobasiert gemäß definiertem Löschkonzept.

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

4.1. Verfügbarkeitskontrolle

- **Hochverfügbarkeit und DDoS-Schutz**: Nutzung von hochverfügbaren Diensten und Schutzmaßnahmen der Cloud-Anbieter.
- **Backup-Konzept**: Regelmäßige Erstellung von verschlüsselten Sicherungskopien gemäß Backup-Konzept.
- **Monitoring**: Angemessene automatisierte Überwachung der Systeme mit definierten Prozessen und Bereitschaften bei kritischen Vorfällen.

4.2. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- **Disaster Recovery Prozesse**: Vorhandensein von Prozessen zur Wiederherstellung im Notfall.
- **Zielwerte**: Es bestehen risikobasierte Zielwerte für RPO (Recovery Point Objective) und RTO (Recovery Time Objective).
- **Wiederherstellungstests**: Regelmäßige Tests der Backup-Integrität und der Wiederherstellungsprozesse.

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

- **Incident Response Management**: Definierte Prozesse für die Erkennung, Analyse, Behebung und Meldung von Sicherheitsvorfällen (inkl. Meldefrist gemäß AVV).
- **Schwachstellenmanagement**: Automatisierte Überprüfung von Code-Abhängigkeiten (Dependency Scanning) und regelmäßiges Vulnerability Scanning. Zeitnahe Implementierung von Sicherheitspatches nach Risikobewertung.
- **Sichere Softwareentwicklung (SSDLC)**: Integration von Sicherheitsaspekten in den Entwicklungsprozess (z.B. Code-Reviews).

- **Sicherheitsüberprüfungen und Tests**: Regelmäßige Sicherheitsüberprüfungen (intern und extern, z.B. Penetrationstests) werden durchgeführt. Nachweise erfolgen gemäß § 9 AVV.
- **Mitarbeiterschulung**: Regelmäßige Sensibilisierung der Mitarbeiter zu Datenschutz und Informationssicherheit.

6. Auftragskontrolle

- **Vertragliche Regelungen**: Klare vertragliche Vereinbarungen (AVV) und Verpflichtung aller Mitarbeiter auf Vertraulichkeit.
- **Sorgfältige Auswahl von Dienstleistern**: Auswahl von Unterauftragsverarbeitern basierend auf Sicherheitsstandards und vertragliche Absicherung (DPAs/AVVs) inklusive Prüfung der Transfermechanismen (TIAs bei Bedarf, vgl. § 7 AVV).
- **Remote-Support**: Remote-Support durch Unterauftragsverarbeiter erfolgt anlassbezogen, unter Einsatz starker Authentifizierung und entsprechender Protokollierung (Audit-Trail).

Anlage 2 zur AVV: Liste der genehmigten Unterauftragsverarbeiter

Zum Zeitpunkt des Abschlusses dieser AVV setzt der Auftragnehmer (Fizard GmbH) die folgenden Unterauftragsverarbeiter ein. Diese gelten als genehmigt. Die geeigneten Garantien richten sich nach § 7 der AVV.

Anbieter (Firma und Anschrift)	**Zweck der Verarbeitung**	**Ort der Verarbeitung (Hosting)**	**Betroffene Datenkategorien**	**Geeignete Garantien (bei Drittlandtransfer)**
Amazon Web Services EMEA SARL (Luxemburg) Mutterkonzern: AWS, Inc. (USA)	Cloud-Infrastruktur (DB, S3), E-Mail-Versand (SES), CDN (CloudFront).	EU (Frankfurt, Deutschland). Remote-Support durch US-Mutter möglich.	Alle Kategorien gemäß § 3 AVV.	EU-US DPF Zertifizierung (AWS, Inc.) (Angemessenheitsbeschluss); Zusätzlich EU-SCCs (Modul 3).
DigitalOcean, LLC (USA)	Cloud-Infrastruktur (Backend-Hosting).	EU (Frankfurt, Deutschland). Remote-Support möglich.	Alle Kategorien gemäß § 3 AVV.	EU-US DPF Zertifizierung (Angemessenheitsbeschluss); Zusätzlich EU-SCCs (Modul 3).
Vercel Inc. (USA)	Frontend-Hosting und Edge Network (CDN).	Globales Netzwerk (CDN).	Nutzungsdaten (IP-Adressen). (Kein Caching personenbezogener Inhalte).	EU-US DPF Zertifizierung (Angemessenheitsbeschluss); Zusätzlich EU-SCCs (Modul 3).
Functional Software, Inc. (Sentry) (USA)	Monitoring, Fehleranalyse (Error Tracking).	EU oder USA (je nach Konfiguration).	Nutzungsdaten; Ggf. minimierte Stamm-/Vertragsdaten (PII-Minimierung implementiert).	EU-US DPF Zertifizierung (Angemessenheitsbeschluss); Zusätzlich EU-SCCs (Modul 3).

Better Stack, Inc. (USA)	Zentrales Log-Management und System-Monitoring.	EU oder USA (je nach Konfiguration).	Nutzungsdaten; System-Logs (PII-Minimierung implementiert).	EU-US DPF Zertifizierung (Angemessenheitsbeschluss); Zusätzlich EU-SCCs (Modul 3).