Auftragsverarbeitungsvertrag (AVV)

Art. 28 Datenschutz-Grundverordnung – DSGVO

Version 1.1 · Stand: November 2026

PARTEIEN

Rolle	Vertragspartei / Identifikation
Dienstleister / Auftragsverarbeiter	flowtax GmbH Rampachertal 1 74076 Heilbronn Geschäftsführung: Rayan Jafarzadeh HRB 803590, Amtsgericht Stuttgart USt-ID: DE460275052 Kontakt: beratung@flowtax.de / info@flowtax.de · Tel.: 07131 3859570
Auftraggeber / Verantwortlicher	Das Unternehmen, das (i) ein Angebot, eine Leistungsbeschreibung oder Order Form des Dienstleisters angenommen hat, (ii) einen Vertrag mit dem Dienstleister geschlossen hat oder (iii) Leistungen des Dienstleisters nutzt und die zugrunde liegenden Bedingungen akzeptiert hat. Die konkrete Identifikation ergibt sich aus Angebot, Auftragsbestätigung, Rechnung, Accountdaten oder sonstigen Vertragsunterlagen, insbesondere juristischer Name, Rechnungs-/Kontaktangaben, Kunden-Nr. oder USt-IdNr.

Hinweis: Dieser AVV ist Bestandteil des jeweiligen Hauptvertrags zwischen den Parteien. Er gilt ausschließlich für Verarbeitungsvorgänge, bei denen flowtax GmbH personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Verarbeitungen, bei denen flowtax GmbH eigenständig Verantwortlicher ist (z. B. eigene Vertragsverwaltung, Rechnungslegung, gesetzliche Aufbewahrung, Marketing gegenüber eigenen Kontakten), sind nicht Gegenstand dieses AVV.

§ 1 Geltungsbereich, Gegenstand und Dauer

(1) Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Dienstleister im Auftrag des Auftraggebers gemäß Art. 28 DSGVO im Zusammenhang mit den beauftragten Leistungen von flowtax GmbH, insbesondere Status-Quo-Analyse, Compliance-Check, Struktur- und Systemaufnahme, Belegfluss-Audit, Schwachstellenanalyse, Handlungsempfehlungen, Change-Management, Erstellung und Pflege von Verfahrensdokumentationen, Prozessdokumentation, Digitalisierungs- und Automatisierungsberatung sowie begleitende Support- und Projektleistungen.

(2) Der konkrete Leistungsumfang ergibt sich aus dem Hauptvertrag, Angebot, Projektauftrag, Statement of Work, der Leistungsbeschreibung oder sonstigen dokumentierten Weisungen des Auftraggebers. Dieser AVV erweitert den Hauptvertrag datenschutzrechtlich; er begründet keine über den Hauptvertrag hinausgehende Leistungspflicht.

(3) Die Laufzeit dieses AVV entspricht der Laufzeit des jeweiligen Hauptvertrags. Er gilt darüber hinaus bis zur vollständigen Löschung, Rückgabe oder zulässigen Archivierung der personenbezogenen Daten gemäß § 10.

(4) Vorrangordnung bei Widersprüchen: (1) Individualabreden, (2) dieser AVV einschließlich **Anlagen**, (3) projektbezogene Leistungsbeschreibung/Order Form, (4) AGB oder sonstige Rahmenbedingungen des Dienstleisters, (5) Hersteller-, Provider- oder Drittanbieterbedingungen, soweit diese wirksam einbezogen wurden.

§ 2 Art, Zwecke und Ort der Verarbeitung

(1) Zwecke der Verarbeitung sind die Durchführung der beauftragten Analyse-, Dokumentations-, Beratungs-, Implementierungs-, Support- und Projektleistungen. Hierzu zählen insbesondere die Aufnahme von Unternehmensstrukturen, IT-Landschaften, Beleg- und Datenflüssen, Prozessrisiken, Compliance-Anforderungen, Schnittstellen, Systemkonfigurationen und Maßnahmenplänen sowie die Erstellung, Pflege oder Übergabe projektbezogener Dokumentationen.

(2) Der Dienstleister kann im Rahmen der Leistungserbringung auf Systeme, Dateien oder Arbeitsumgebungen des Auftraggebers zugreifen, insbesondere Rechnungswesen-/Buchhaltungsumgebungen, DATEV-Umgebungen, ERP/WaWi/CRM-Systeme, DMS/Archivsysteme, Microsoft 365, SharePoint/OneDrive, E-Mail-Postfächer, Belegplattformen, Kollaborationstools, Prozessmanagement- und Dokumentationssysteme.

Einsichtnahmen in Inhaltsdaten erfolgen nur zweckgebunden und soweit für die Auftragsdurchführung erforderlich oder vom Auftraggeber angewiesen.

(3) Verarbeitungsvorgänge können insbesondere sein: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung innerhalb beauftragter Systeme, Abgleichen, Einschränken, Löschen und Vernichten personenbezogener Daten.

(4) Verarbeitungsorte liegen grundsätzlich in der EU/im EWR. Drittlandbezüge aufgrund eingesetzter Hersteller, Cloud-, SaaS- oder Supportanbieter sind nach Maßgabe von § 12 und **Anlage B** zulässig.

§ 3 Datenarten und betroffene Personen

(1) Datenarten können insbesondere sein: Identitäts- und Kontaktdaten, Benutzer- und Berechtigungsdaten, Kommunikationsdaten, Vertrags-, Projekt- und Abrechnungsdaten, System- und Protokolldaten, Prozess- und Organisationsdaten, Belege, Rechnungen, Buchhaltungs-, Finanz-, Zahlungs- und Steuerdaten, Kunden-/Lieferantenstammdaten des Auftraggebers, Dokumentationsinhalte, Maßnahmenpläne, Schnittstelleninformationen sowie ggf. HR-, Lohn- oder Beschäftigtendaten, sofern diese vom Auftraggeber bereitgestellt oder für die beauftragte Analyse erforderlich sind.

(2) Betroffene Personen können insbesondere sein: Geschäftsführung, Mitarbeitende, Administratoren, Nutzer und Ansprechpartner des Auftraggebers, Kunden, Lieferanten, Dienstleister, Berater, Steuerberater, Wirtschaftsprüfer, sonstige Geschäftspartner des Auftraggebers sowie Personen, deren Daten in Belegen, Buchhaltungsunterlagen, E-Mails oder Systemen des Auftraggebers enthalten sind.

(3) Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten nach Art. 10 DSGVO sind nicht Gegenstand einer gezielten Verarbeitung durch den Dienstleister. Eine anlassbezogene Kenntnisnahme kann jedoch nicht ausgeschlossen werden, etwa in Belegen, E-Mails, Lohnunterlagen oder sonstigen Kundendokumenten. Der Auftraggeber informiert den Dienstleister vorab, wenn derartige Daten typischerweise Gegenstand des Projekts sind; die Parteien vereinbaren erforderlichenfalls zusätzliche Schutzmaßnahmen.

§ 4 Weisungen

(1) Der Dienstleister verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Weisungen können sich aus Hauptvertrag, Leistungsbeschreibung, Ticket, E-Mail, Projektprotokoll, Freigabe, Systemberechtigung oder sonstiger Textform ergeben.

(2) Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen. Der Dienstleister darf eine mündliche Weisung ausführen, wenn sie zur ordnungsgemäßen Leistungserbringung erforderlich erscheint und keine Anhaltspunkte für eine Rechtswidrigkeit bestehen.

(3) Hält der Dienstleister eine Weisung für rechtswidrig oder offensichtlich unzweckmäßig, informiert er den Auftraggeber unverzüglich. Die Durchführung der Weisung kann bis zur Klärung ausgesetzt werden, soweit hierdurch keine dringenden Schutz- oder Sicherungsmaßnahmen verhindert werden.

§ 5 Vertraulichkeit und Verschwiegenheit

(1) Der Dienstleister verpflichtet alle mit der Verarbeitung personenbezogener Daten befassten Personen zur Vertraulichkeit, soweit keine gesetzliche Verschwiegenheitspflicht besteht. Die Verpflichtung umfasst personenbezogene Daten, Geschäfts- und Betriebsgeheimnisse, steuerrelevante Informationen, Prozessdokumentationen, Zugangsdaten, Systemarchitekturen sowie sonstige vertrauliche Informationen des Auftraggebers.

(2) Die eingesetzten Personen werden angemessen zu Datenschutz, Informationssicherheit und vertraulichem Umgang mit Kundendaten sensibilisiert.

(3) Die Vertraulichkeitspflichten bestehen über das Ende des Hauptvertrags und dieses AVV hinaus fort.

§ 6 Technische und organisatorische Maßnahmen (TOM)

(1) Der Dienstleister unterhält angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die zum Zeitpunkt des Vertragsschlusses geltenden Baseline-Maßnahmen sind in **Anlage A** beschrieben.

(2) Baseline-Maßnahmen umfassen insbesondere rollenbasierte Zugriffsbeschränkungen nach dem Need-to-know- und Least-Privilege-Prinzip, Multi-Faktor-Authentisierung für administrative und kritische Zugänge,

Verschlüsselung bei Übertragung und soweit möglich bei Speicherung, sichere Endgeräte, Patch- und Schwachstellenmanagement, Protokollierung relevanter administrativer Aktivitäten, gesicherte Remote-Zugriffe, geregelte Löschung/Rückgabe von Daten sowie Incident-Response-Prozesse.

(3) Der Dienstleister darf TOM an technische und organisatorische Entwicklungen anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die das Risiko für die Rechte und Freiheiten betroffener Personen erhöhen können, werden dem Auftraggeber angemessen mitgeteilt.

(4) Der Auftraggeber erhält auf Anfrage geeignete Nachweise zu den TOM, soweit dadurch keine Sicherheits-, Geheimhaltungs- oder Rechte Dritter beeinträchtigt werden.

§ 7 Unterauftragsverhältnisse

(1) Der Dienstleister darf Unterauftragsverarbeiter einsetzen, soweit dies zur Erbringung der vertraglichen Leistungen erforderlich ist. Eine aktuelle oder initiale Übersicht ergibt sich aus **Anlage B**. Vom Auftraggeber bereitgestellte Systeme und Provider, bei denen der Auftraggeber selbst Vertragsinhaber ist, gelten nicht als Unterauftragsverarbeiter des Dienstleisters.

(2) Der Dienstleister verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die dem Schutzniveau dieses AVV im Wesentlichen entsprechen, insbesondere gemäß Art. 28 Abs. 4 DSGVO. Der Dienstleister prüft die Angemessenheit der vom Unterauftragsverarbeiter getroffenen Schutzmaßnahmen risikobasiert.

(3) Änderungen oder Ergänzungen der Unterauftragsverarbeiterliste teilt der Dienstleister dem Auftraggeber in geeigneter Weise mit. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von zehn (10) Werktagen widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

(4) Der Dienstleister bleibt gegenüber dem Auftraggeber für die ordnungsgemäße Verarbeitung durch Unterauftragsverarbeiter verantwortlich.

§ 8 Unterstützungspflichten

(1) Der Dienstleister unterstützt den Auftraggeber im erforderlichen und zumutbaren Umfang bei der Erfüllung datenschutzrechtlicher Pflichten, insbesondere bei Betroffenenrechten nach Art. 12 bis 23 DSGVO, Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO, vorherigen Konsultationen nach Art. 36 DSGVO sowie bei Meldungen und Benachrichtigungen nach Art. 33 und 34 DSGVO.

(2) Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung, Rechtsgrundlagen, Informationspflichten, Interessenabwägungen, Löschfristen, Verzeichnisse von Verarbeitungstätigkeiten sowie die Bearbeitung von Betroffenenanfragen verantwortlich.

(3) Unterstützungsleistungen, die über vertraglich geschuldete Standardleistungen hinausgehen, werden nach Aufwand vergütet, sofern der Aufwand nicht durch einen vom Dienstleister zu vertretenden Verstoß verursacht wurde.

§ 9 Meldung von Datenschutzverletzungen

(1) Der Dienstleister meldet dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Bekanntwerden, soweit die Verletzung Daten betrifft, die im Auftrag des Auftraggebers verarbeitet werden.

(2) Die Meldung enthält, soweit verfügbar, Angaben zu Art und Umfang der Verletzung, betroffenen Daten und Personengruppen, wahrscheinlichen Folgen, bereits ergriffenen oder vorgeschlagenen Maßnahmen sowie Ansprechpartnern für Rückfragen.

(3) Fehlende Informationen werden nachgereicht, sobald sie dem Dienstleister mit vertretbarem Aufwand zur Verfügung stehen. Der Auftraggeber bleibt für Meldungen an Aufsichtsbehörden und Benachrichtigungen betroffener Personen verantwortlich.

§ 10 Löschung, Rückgabe und Offboarding

(1) Nach Abschluss der Leistung, Vertragsende oder auf dokumentierte Weisung des Auftraggebers löscht der Dienstleister personenbezogene Daten oder gibt sie in einem gängigen Format zurück, sofern keine gesetzlichen Aufbewahrungspflichten, Nachweispflichten oder berechtigten Sicherungszwecke entgegenstehen.

(2) Offboarding-Maßnahmen können insbesondere umfassen: Übergabe von Dokumentationen, Export projektbezogener Dateien, Entzug oder Deaktivierung von Zugriffsrechten, Übergabe relevanter Konfigurationsinformationen, Löschung temporärer Arbeitskopien sowie Bestätigung der Löschung auf Anfrage.

(3) Sofern nichts Abweichendes vereinbart ist, erfolgt die Rückgabe oder Löschung innerhalb von 30 Kalendertagen nach Vertragsende oder entsprechender Weisung. Backup-, Log- und Archivdaten werden im Rahmen regulärer Löschzyklen gelöscht, soweit keine frühere Löschung technisch möglich und zumutbar ist.

§ 11 Nachweise und Audits

(1) Der Dienstleister stellt dem Auftraggeber auf Anfrage geeignete Nachweise zur Einhaltung dieses AVV zur Verfügung, etwa TOM-Beschreibungen, Prozessbeschreibungen, Zertifikate, Provider-Nachweise oder Selbstauskünfte.

(2) Audits oder Inspektionen durch den Auftraggeber oder einen zur Verschwiegenheit verpflichteten Prüfer sind nach angemessener Vorankündigung und Abstimmung möglich. Betriebs- und Sicherheitsinteressen des Dienstleisters, Rechte anderer Kunden sowie Geheimhaltungsinteressen sind zu wahren.

(3) Vor-Ort-Audits sind auf das erforderliche Maß zu beschränken und dürfen den Geschäftsbetrieb des Dienstleisters nicht unverhältnismäßig beeinträchtigen. Mehraufwände trägt der Auftraggeber, sofern kein begründeter Verdacht auf einen Datenschutzverstoß des Dienstleisters besteht.

§ 12 Datenübermittlungen in Drittländer

(1) Eine Übermittlung personenbezogener Daten in Staaten außerhalb der EU/des EWR oder an internationale Organisationen erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Soweit Unterauftragsverarbeiter oder Hersteller Dienste mit Drittlandbezug erbringen, stellt der Dienstleister risikobasiert sicher, dass geeignete Transferinstrumente bestehen, insbesondere Angemessenheitsbeschluss, EU-Standardvertragsklauseln, ergänzende Schutzmaßnahmen oder sonstige zulässige Garantien.

(3) Einzelheiten ergeben sich aus **Anlage B** und den jeweils geltenden Datenschutz- und Vertragsdokumenten der eingesetzten Provider.

§ 13 Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO. Er ist für die Zulässigkeit der Verarbeitung, die Rechtmäßigkeit der bereitgestellten Daten, Transparenzpflichten gegenüber betroffenen Personen, die Vergabe von Berechtigungen, die Richtigkeit der Weisungen und die Definition erforderlicher Lösch- und Aufbewahrungsfristen verantwortlich.

(2) Der Auftraggeber stellt sicher, dass dem Dienstleister nur solche Daten zugänglich gemacht werden, die für die beauftragten Leistungen erforderlich sind. Er hält Benutzerkonten, Systemzugänge, Freigaben, Ansprechpartner, Domänen, Datenräume und Berechtigungskonzepte aktuell und informiert den Dienstleister unverzüglich über sicherheitsrelevante Änderungen.

(3) Der Auftraggeber bleibt verantwortlich für seine eigenen Backups, Archivierung, Revisionssicherheit, GoBD-Umsetzung und gesetzlichen Aufbewahrungspflichten, sofern diese Leistungen nicht ausdrücklich und schriftlich beim Dienstleister beauftragt sind.

§ 14 Einsatz von KI-, Analyse- und Automatisierungswerkzeugen

(1) Soweit im Rahmen der beauftragten Leistungen KI-, Analyse- oder Automatisierungswerkzeuge eingesetzt werden, erfolgt dies nur zweckgebunden, risikobasiert und im Rahmen dokumentierter Weisungen des Auftraggebers. Dies gilt insbesondere für Prozessanalysen, Dokumentationsentwürfe, Workflow-Automatisierungen, Klassifizierungen, Datenstrukturierungen oder technische Assistenzsysteme.

(2) Personenbezogene Produktivdaten werden in externen KI-/Analysewerkzeugen grundsätzlich nicht eingesetzt, sofern der Auftraggeber dies nicht ausdrücklich freigibt oder die Verarbeitung durch **Anlage B** sowie die jeweilige Leistungsbeschreibung abgedeckt ist. Wo möglich, sind anonymisierte, pseudonymisierte oder abstrahierte Testdaten zu verwenden.

(3) Der Dienstleister stellt sicher, dass eingesetzte KI-/Analyseanbieter, soweit sie als Unterauftragsverarbeiter tätig werden, in **Anlage B** aufgenommen und datenschutzrechtlich angemessen verpflichtet werden.

§ 15 Berufsgeheimnisse, Steuer- und Geschäftsgeheimnisse

(1) Soweit der Auftraggeber oder dessen Kunden berufsrechtlichen, steuerlichen, handelsrechtlichen oder sonstigen Verschwiegenheitspflichten unterliegen und dem Dienstleister entsprechende Daten zugänglich machen, behandelt der Dienstleister diese Informationen mit besonderer Vertraulichkeit und begrenzt Zugriffe nach dem Need-to-know-Prinzip.

(2) Der Dienstleister verarbeitet steuerrelevante Belege, Buchführungsdaten, Verfahrensdokumentationen, interne Prozessbeschreibungen, Geschäftsgeheimnisse und Systeminformationen ausschließlich zur Leistungserbringung und nicht zu eigenen Zwecken.

(3) Unterauftragsverarbeiter werden nur eingesetzt, soweit dies zur Leistungserbringung erforderlich ist und die Anforderungen dieses AVV eingehalten werden. Soweit eine vorherige Zustimmung oder besondere Information des Auftraggebers erforderlich ist, wird diese eingeholt.

§ 16 Haftung und Vergütung

(1) Die Haftung der Parteien richtet sich nach den Regelungen des Hauptvertrags und den gesetzlichen Bestimmungen. Zwingende gesetzliche Haftungstatbestände, insbesondere für Leben, Körper, Gesundheit, Vorsatz, grobe Fahrlässigkeit, Garantie, Arglist und Produkthaftung, bleiben unberührt.

(2) Unterstützungs-, Audit-, Export-, Sonderlöschungs- oder Zusatzaufwände nach diesem AVV werden nach den im Hauptvertrag vereinbarten Sätzen vergütet, sofern der Aufwand nicht durch einen vom Dienstleister zu vertretenden Pflichtverstoß verursacht wurde.

§ 17 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses AVV bedürfen mindestens der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist.

(2) Es gilt deutsches Recht. Gerichtsstand richtet sich nach dem Hauptvertrag, sofern gesetzlich zulässig.

(3) Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Anstelle der unwirksamen Bestimmung gilt die gesetzliche Regelung; die Parteien werden eine wirtschaftlich möglichst nahekommende, wirksame Regelung vereinbaren.

Gültigkeit

Dieser AVV kann elektronisch, in Textform oder handschriftlich unterzeichnet werden, soweit der Hauptvertrag keine strengere Form vorsieht.

ANLAGE A – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

Die folgenden Maßnahmen bilden die Baseline des Dienstleisters. Konkrete Projektausprägungen können je nach beauftragtem Leistungsumfang, eingesetzten Kundensystemen und vereinbarten Toolchains variieren.

A1 Governance & Verantwortlichkeiten

- Datenschutz- und Informationssicherheitsverantwortlichkeiten sind intern zugeordnet.
- Richtlinien und Arbeitsanweisungen werden risikobasiert überprüft und aktualisiert.
- Owner: Geschäftsführung/IT-Verantwortliche | Prüfintervall: jährlich

A2 Vertraulichkeit & Awareness

- Mitarbeitende und eingesetzte Personen werden auf Vertraulichkeit verpflichtet.
- Regelmäßige Sensibilisierung zu Datenschutz, Phishing, Geheimnisschutz und sicherem Umgang mit Kundendaten.
- Owner: Geschäftsführung | Prüfintervall: jährlich

A3 Identitäten & Zugriffssteuerung

- Rollen- und Berechtigungskonzepte nach Need-to-know/Least-Privilege.
- MFA für administrative und kritische Zugänge, soweit technisch verfügbar.
- Regelmäßige Überprüfung aktiver Zugänge und Entzug nicht mehr benötigter Rechte.
- Owner: IT-Verantwortliche | Prüfintervall: halbjährlich

A4 Kundenzugriffe & Remote-Arbeit

- Zugriffe auf Kundensysteme nur auf Weisung, projektbezogen und zweckgebunden.
- Remote-Zugriffe über gesicherte Verbindungen oder freigegebene Kundentools.
- Sitzungen und wesentliche administrative Tätigkeiten werden angemessen dokumentiert.
- Owner: Projektleitung/IT | Prüfintervall: laufend

A5 Endgeräte & Arbeitsplatzsicherheit

- Geschäftlich genutzte Geräte mit Zugriffsschutz, Bildschirmsperre und aktueller Sicherheitssoftware.
- Betriebssysteme und Anwendungen werden regelmäßig aktualisiert.
- Speicherung lokaler Arbeitskopien wird auf das erforderliche Maß begrenzt.
- Owner: IT-Verantwortliche | Prüfintervall: quartalsweise

A6 Verschlüsselung & sichere Übertragung

- Transportverschlüsselung (TLS/HTTPS) für Übertragungen, soweit technisch möglich.
- Verschlüsselung ruhender Daten durch eingesetzte Plattformen, Cloud- oder Endgerätefunktionen, soweit verfügbar.
- Passwörter, Tokens und Geheimnisse werden getrennt und geschützt verwaltet.
- Owner: IT-Verantwortliche | Prüfintervall: halbjährlich

A7 Datenminimierung & Zweckbindung

- Es werden nur Daten verarbeitet, die für Analyse, Dokumentation, Support oder Umsetzung erforderlich sind.
- Arbeitskopien, Exporte und Downloads werden auf erforderliche Zwecke beschränkt.
- Personenbezogene Produktivdaten in Test-/Demo-/KI-Umgebungen nur bei Freigabe oder Weisung.
- Owner: Projektleitung | Prüfintervall: je Projekt

A8 Logging & Nachvollziehbarkeit

- Relevante administrative Aktivitäten werden soweit verhältnismäßig protokolliert.
- Projektentscheidungen, Freigaben und Weisungen werden in geeigneten Projektunterlagen dokumentiert.
- Log-Aufbewahrung erfolgt risikobasiert und im Rahmen der eingesetzten Systeme.
- Owner: IT/Projektleitung | Prüfintervall: monatlich Sichtkontrolle

A9 Patch- & Schwachstellenmanagement

- Sicherheitsupdates werden risikobasiert eingespielt.
- Kritische Schwachstellen werden priorisiert behandelt.
- Eingesetzte SaaS-/Cloud-Anbieter werden anhand verfügbarer Sicherheitsinformationen bewertet.
- Owner: IT-Verantwortliche | Prüfintervall: monatlich

A10 Backup & Wiederherstellung

- Backups eigener Arbeitsumgebungen erfolgen entsprechend interner Betriebsanforderungen.
- Kundenseitige Backup- oder Archivpflichten bestehen nur, wenn sie ausdrücklich beauftragt sind.
- Wiederherstellungsfähigkeit beauftragter Backup-Leistungen wird angemessen getestet.
- Owner: IT-Verantwortliche | Prüfintervall: nach Leistungsumfang

A11 Incident Response

- Verdachtsfälle und Sicherheitsvorfälle werden intern eskaliert und bewertet.

- Meldung an den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, soweit Kundendaten betroffen sind.
- Lessons Learned und risikobasierte Folgeverbesserungen nach relevanten Vorfällen.
- Owner: Geschäftsführung/IT | Prüfintervall: jährlich Übung/Review

A12 Lieferanten- und Sub-AV-Management

- Sub-Auftragsverarbeiter werden risikobasiert ausgewählt und vertraglich verpflichtet.
- DPA/Sub-AV-Unterlagen, TOM und ggf. Drittlandtransfergrundlagen werden angemessen geprüft.
- Änderungen werden dem Auftraggeber mit Widerspruchsmöglichkeit mitgeteilt.
- Owner: Geschäftsführung/IT | Prüfintervall: jährlich

A13 Mandanten- und Projekttrennung

- Projekt- und Kundendaten werden organisatorisch und soweit möglich technisch getrennt.
- Zugriffe auf Projekträume, Datenräume und Dokumentationen werden kundenspezifisch beschränkt.
- Nach Projektabschluss werden Berechtigungen überprüft und nicht mehr erforderliche Arbeitsstände gelöscht oder archiviert.
- Owner: Projektleitung | Prüfintervall: je Projektabschluss

A14 Privacy by Design/Default

- Prozess- und Dokumentationslösungen werden mit Fokus auf Datenminimierung, Zugriffsbeschränkung und Löschbarkeit konzipiert.
- Empfehlungen an Auftraggeber berücksichtigen datenschutzfreundliche Voreinstellungen und revisionssichere, nachvollziehbare Abläufe.
- Owner: Projektleitung/Datenschutzverantwortliche | Prüfintervall: je Projekt

ANLAGE B – UNTERAUFTRAGSVERARBEITER / PROVIDER

Stand: November 2026. Der Dienstleister setzt die folgenden Unterauftragsverarbeiter ein. Änderungen werden gemäß § 7 Abs. 3 mitgeteilt.

Anbieter (Firma, Sitz)	Zweck / Leistung	Datenkategorien	Verarbeitungsort / Drittland	Einsatz
Microsoft Ireland Operations Ltd., Dublin, Irland (Microsoft 365)	E-Mail, Teams, SharePoint/OneDrive, ggf. Kundendatenräume	Kontakt-, Kommunikations-, Projekt-, Dokumentations- und Inhaltsdaten	EU/EWR; Supportzugriff aus den USA möglich (EU-US DPF, Standardvertragsklauseln)	ständig
smartdocu Solutions GmbH, Chieming (HRB 28577, AG Traunstein)	Bereitstellung, Betrieb und Support der VFD-Software für die Plattform vfd.flowtax.de	Verfahrensdokumentations-, Prozess-, Benutzer- und Protokolldaten	Deutschland	ständig, für Nutzer der VFD-Plattform
Hetzner Online GmbH, Gunzenhausen (HRB 6089, AG Ansbach)	Serverhosting der Plattform vfd.flowtax.de	Verfahrensdokumentations-, Prozess-, Benutzer- und Protokolldaten	Deutschland (Rechenzentrum Hetzner)	ständig, für Nutzer der VFD-Plattform
RGJ Web & IT Solutions GmbH, Lauffen am Neckar	IT-Betreuung, Administration und Wartung der IT-Systeme des Dienstleisters	System-, Protokoll- und ggf. Inhaltsdaten im Rahmen der Wartung	Deutschland	ständig
Microsoft Ireland Operations Ltd., Dublin, Irland (Microsoft OneDrive)	Datenablage und Datensicherung der eigenen Arbeitsumgebung	Projekt-, Dokumentations- und Inhaltsdaten	EU/EWR; Supportzugriff aus den USA möglich (EU-US DPF, Standardvertragsklauseln)	ständig
Anthropic Ireland, Limited, Dublin, Irland (Claude)	Analyse, Strukturierung und Entwurfsunterstützung nach § 14	Nur freigegebene, möglichst anonymisierte oder pseudonymisierte Daten	USA möglich (EU-US DPF, Standardvertragsklauseln)	nur nach Freigabe durch den Auftraggeber
OpenAI Ireland Ltd., Dublin, Irland (ChatGPT)	Analyse, Strukturierung und Entwurfsunterstützung nach § 14	Nur freigegebene, möglichst anonymisierte oder pseudonymisierte Daten	USA möglich (EU-US DPF, Standardvertragsklauseln)	nur nach Freigabe durch den Auftraggeber
Google Ireland Limited, Dublin, Irland (Gemini)	Analyse, Strukturierung und Entwurfsunterstützung nach § 14	Nur freigegebene, möglichst anonymisierte oder pseudonymisierte Daten	USA möglich (EU-US DPF, Standardvertragsklauseln)	nur nach Freigabe durch den Auftraggeber

Hinweis: DATEV, ERP-, DMS-, CRM-, WaWi-, E-Mail- oder Archivsysteme des Auftraggebers gelten nicht als Unterauftragsverarbeiter des Dienstleisters, wenn der Auftraggeber oder ein Dritter Vertragsinhaber dieser Systeme ist und flowtax GmbH lediglich auf Weisung im Kundensystem arbeitet.

ANLAGE C – BESCHREIBUNG DER VERARBEITUNG

Kriterium	Beschreibung
Gegenstand	Verarbeitung personenbezogener Daten im Rahmen von Prozess-, Compliance-, GoBD-, Verfahrensdokumentations-, Digitalisierungs- und Automatisierungsprojekten sowie begleitenden Supportleistungen.
Dauer	Laufzeit des Hauptvertrags zzgl. Offboarding-, Rückgabe-, Lösch- und gesetzlicher Aufbewahrungszeiträume.
Art der Verarbeitung	Erheben, Erfassen, Ordnen, Speichern, Auslesen, Strukturieren, Analysieren, Dokumentieren, Übermitteln innerhalb beauftragter Systeme, Löschen, Vernichten.
Zwecke	Analyse der Ist-Prozesse, Dokumentation von Belegflüssen und IT-Landschaften, Identifikation von Schwachstellen, Ableitung von Handlungsempfehlungen, Erstellung/Pflege von Verfahrensdokumentationen, Implementierungs- und Change-Unterstützung.
Datenarten	Identitäts-, Kontakt-, Benutzer-, Kommunikations-, Vertrags-, Projekt-, System-, Protokoll-, Finanz-, Buchhaltungs-, Steuer-, Beleg-, Prozess-, Organisations- und ggf. HR-/Lohndaten.
Betroffene Personen	Mitarbeitende, Nutzer, Administratoren, Geschäftsführung, Kunden, Lieferanten, Dienstleister, Berater und sonstige Ansprechpartner des Auftraggebers sowie Personen in Belegen oder Systemen des Auftraggebers.
Verantwortlichkeit	Auftraggeber = Verantwortlicher; flowtax GmbH = Auftragsverarbeiter, soweit Verarbeitung im Auftrag erfolgt.
Besondere Hinweise	Besondere Kategorien personenbezogener Daten sind nicht gezielt Gegenstand der Verarbeitung, können aber anlassbezogen in Belegen, E-Mails oder Lohn-/HR-Unterlagen enthalten sein.

ANLAGE D – KUNDENSEITIGE MINDESTMITWIRKUNG

- Benennung fachlicher und technischer Ansprechpartner mit Entscheidungs- und Weisungsbefugnis.
- Bereitstellung erforderlicher Systemzugänge nach Least-Privilege, möglichst zeitlich befristet.
- Bereitstellung relevanter Prozess-, System-, Belegfluss- und Organisationsinformationen.

- Freigabe von Datenräumen, Exporten, Screenshots, Prozessaufnahmen und Dokumentationsständen.
- Kennzeichnung besonders schutzwürdiger Datenbestände und rechtzeitige Information über Berufsgeheimnisse, Art.-9- oder Art.-10-Daten.
- Prüfung und Freigabe von Handlungsempfehlungen, Verfahrensdokumentationen und Maßnahmenplänen vor produktiver Nutzung