Auftragsverarbeitungsvertrag

nach Art. 28 DSGVO

Fassung 2026-10 · Stand 23. Oktober 2026

Fassung	Stand	Änderung
2026-10	2026-10-23	Erste veröffentlichte Fassung.

Vertragsparteien

DID Daten-Intermediär-Dienste FlexCo, FN 637970 t, Treustraße 52, 1200 Wien, Österreich, office@intermediary.at – nachfolgend „DID FlexCo“ oder „Auftragsverarbeiter“ –

und

der Organisation, die die Dienste von DID FlexCo nutzt – nachfolgend „Verantwortlicher“ –

gemeinsam auch die „Parteien“.

Der Verantwortliche ist die auf der Plattform von DID FlexCo registrierte Organisation. Seine Identifikationsangaben ergeben sich aus der von ihm bestätigten Selbsterklärung und aus dem jeweiligen Hauptvertrag.

1. Gegenstand und Dauer der Verarbeitung

Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch DID FlexCo im Auftrag des Verantwortlichen im Rahmen der Bereitstellung neutraler Datenintermediär-Dienste. Dieser Vertrag ergänzt die Allgemeinen Geschäftsbedingungen von DID FlexCo sowie sonstige zwischen den Parteien geschlossene Verträge (gemeinsam die „Hauptverträge“) und regelt die datenschutzrechtlichen Anforderungen an diese Verarbeitung.

Die Verarbeitung erfolgt für die Dauer des zugrundeliegenden Hauptvertrags und darüber hinaus nur, soweit gesetzliche Aufbewahrungspflichten bestehen.

Für die Zwecke dieses Vertrags gelten die Begriffsbestimmungen der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO).

2. Art, Zweck und Rechtsgrundlage der Verarbeitung

Zweck der Verarbeitung ist ausschließlich die technische und organisatorische Durchführung der vom Verantwortlichen festgelegten Datenweitergabe und der von ihm beauftragten unterstützenden Leistungen. DID FlexCo verfolgt keine eigenen Verarbeitungszwecke.

Die Festlegung der Rechtsgrundlage für die Verarbeitung obliegt ausschließlich dem Verantwortlichen. DID FlexCo verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf die Übermittlung in ein Drittland, es sei denn, sie ist dazu nach dem Recht der Union oder eines Mitgliedstaats verpflichtet; in diesem Fall teilt sie dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3. Kategorien personenbezogener Daten und betroffener Personen

Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien personenbezogener Daten und betroffener Personen ergeben sich aus Anhang 1. DID FlexCo verarbeitet nur die Kategorien von Daten, die durch den Verantwortlichen vorgegeben werden.

Eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist nicht vorgesehen. Werden solche Daten ausnahmsweise verarbeitet, erfolgt dies ausschließlich auf dokumentierte Weisung des Verantwortlichen und unter Einhaltung der gesetzlichen Voraussetzungen.

4. Pflichten von DID FlexCo

4.1 Weisungsbindung

DID FlexCo verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Die Weisungen umfassen insbesondere die vom Verantwortlichen festgelegten Zwecke der Datenweitergabe, die ausgewählten Datenkategorien, die vorgesehenen Empfänger, die Dauer der Bereitstellung sowie die vom Verantwortlichen veranlassten Löschungs-, Rückgabe- oder Einschränkungsmaßnahmen.

Erkennt DID FlexCo, dass eine Weisung gegen geltendes Datenschutzrecht verstößt, informiert sie den Verantwortlichen unverzüglich.

4.2 Vertraulichkeit

DID FlexCo stellt sicher, dass alle mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet sind und regelmäßig datenschutzrechtlich geschult werden. Die Verschwiegenheitsverpflichtung bleibt auch nach Beendigung der Tätigkeit und nach dem Ausscheiden aus DID FlexCo aufrecht.

4.3 Technische und organisatorische Maßnahmen

DID FlexCo ergreift geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die Maßnahmen sind in Anhang 2 beschrieben und Bestandteil dieses Vertrags. Die Maßnahmen umfassen, soweit für die konkrete Verarbeitung erforderlich, insbesondere Zugangskontrollen, Berechtigungskonzepte, Verschlüsselung, Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellungsverfahren, Protokollierung, Trennung von Datenbeständen, Löschverfahren sowie Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der Maßnahmen.

DID FlexCo überprüft die Maßnahmen regelmäßig und passt sie bei Bedarf an den Stand der Technik, die Art der Verarbeitung und die erkennbaren Risiken an. Wesentliche Änderungen der Maßnahmen werden dem Verantwortlichen mitgeteilt; das erreichte Schutzniveau wird dabei nicht unterschritten.

4.4 Unterstützungspflichten

DID FlexCo unterstützt den Verantwortlichen unverzüglich bei der Wahrnehmung der Rechte betroffener Personen nach Art. 12 bis 23 DSGVO und stellt dafür die erforderlichen Informationen, Daten und Unterlagen bereit, soweit dies technisch und organisatorisch zumutbar ist. Richtet eine betroffene Person einen Antrag unmittelbar an DID FlexCo, leitet DID FlexCo diesen unverzüglich an den Verantwortlichen weiter.

Darüber hinaus unterstützt DID FlexCo den Verantwortlichen bei der Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei Datenschutz-Folgenabschätzungen und bei vorherigen Konsultationen.

4.5 Meldung von Verletzungen des Schutzes personenbezogener Daten

DID FlexCo meldet dem Verantwortlichen jede ihr bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden ab Kenntnis (Art. 33 Abs 2 DSGVO). Die Meldung enthält, soweit verfügbar, die in Art. 33 Abs 3 DSGVO genannten Angaben; fehlende Angaben werden ohne unangemessene weitere Verzögerung nachgereicht.

DID FlexCo unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO und dokumentiert jede Verletzung einschließlich der damit verbundenen Tatsachen, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen.

4.6 Rückgabe und Löschung von Daten

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht DID FlexCo die personenbezogenen Daten oder gibt sie zurück. Die Wahl zwischen Löschung und Rückgabe trifft der Verantwortliche (Art. 28 Abs 3 lit g DSGVO); trifft er bis zum Vertragsende keine Wahl, werden die Daten gelöscht.

Die Rückgabe erfolgt in einem strukturierten, gängigen und maschinenlesbaren Format über die Plattform oder eine Schnittstelle. Die Löschung erfolgt innerhalb von höchstens 30 Tagen nach Weisung oder Vertragsende aus den produktiven Systemen. Sicherungskopien werden im Rahmen der festgelegten Backup-Zyklen gelöscht und bis dahin gegen reguläre Nutzung geschützt. Gesetzliche Aufbewahrungspflichten bleiben unberührt; die betroffenen Daten werden in diesem Fall ausschließlich zu Aufbewahrungszwecken verarbeitet. Auf Verlangen weist DID FlexCo die Löschung nach.

4.7 Fortführung des Dienstes und Verfügbarkeit der Daten

DID FlexCo hält technische und organisatorische Vorkehrungen bereit, die eine angemessene Fortführung ihres Datenintermediationsdienstes sicherstellen und es dem Verantwortlichen ermöglichen, die bei DID FlexCo gespeicherten Daten abzurufen, zu übertragen oder herunterzuladen, auch im Fall der Zahlungsunfähigkeit oder der Einstellung des Dienstes (Art. 12 lit h der Verordnung (EU) 2022/868).

Eine beabsichtigte Einstellung des Dienstes teilt DID FlexCo dem Verantwortlichen mindestens drei Monate im Voraus mit. Bis zum Ablauf dieser Frist bleiben Abruf und Übertragung der Daten möglich. Unabhängig davon kann der Verantwortliche die bei DID FlexCo gespeicherten Daten jederzeit über die Plattform und deren Schnittstelle exportieren, sodass der Zugang zu den Daten nicht vom Fortbestand von DID FlexCo abhängt.

4.8 Nachweis- und Kontrollrechte

DID FlexCo stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus diesem Vertrag zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen (Art. 28 Abs 3 lit h DSGVO).

Die Überprüfung erfolgt vorrangig durch Dokumentenprüfung, Selbstauskunft oder durch Vorlage vorhandener Zertifikate und Prüfberichte. Der Verantwortliche kann bei Bedarf und insbesondere bei begründeten Zweifeln zusätzliche Prüfungen einschließlich Vor-Ort-Inspektionen selbst oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen lassen. Prüfungen erfolgen nach angemessener Vorankündigung, zu üblichen Geschäftszeiten und unter Berücksichtigung berechtigter Sicherheits- und Betriebsinteressen von DID FlexCo.

5. Neutralität und Rollenabgrenzung

DID FlexCo agiert als neutraler Datenintermediär. Sie nutzt die Daten nicht für eigene Zwecke, erstellt keine Profile, führt keine Analyse, Aggregation oder Vermarktung durch und trifft keine eigenständigen Entscheidungen über Zwecke oder Mittel der Verarbeitung.

Für Daten, die DID FlexCo zur Erfüllung eigener gesetzlicher oder vertraglicher Pflichten verarbeitet, insbesondere Identitäts-, Vertrags- und Protokolldaten, ist DID FlexCo selbst Verantwortliche. Die entsprechenden Informationen ergeben sich aus ihrer Datenschutzinformation.

6. Subauftragsverarbeiter

Der Verantwortliche erteilt DID FlexCo die allgemeine schriftliche Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter (Art. 28 Abs 2 DSGVO). Die zum Zeitpunkt des Vertragsabschlusses eingesetzten Subauftragsverarbeiter ergeben sich aus Anhang 3.

DID FlexCo informiert den Verantwortlichen mindestens 30 Tage vor jeder beabsichtigten Hinzuziehung oder Ersetzung eines Subauftragsverarbeiters in Textform oder über die Plattform. Der Verantwortliche kann der Änderung innerhalb dieser Frist aus wichtigem Grund widersprechen. Kommt keine Einigung zustande, kann jede Partei den betroffenen Hauptvertrag mit angemessener Frist beenden.

Beauftragt DID FlexCo einen Subauftragsverarbeiter, verpflichtet sie ihn vertraglich zu denselben Datenschutzpflichten, die DID FlexCo nach diesem Vertrag treffen, insbesondere hinsichtlich Weisungsbindung, technischer und organisatorischer Maßnahmen und Unterstützungspflichten. Der Vertrag muss hinreichende Garantien für eine Verarbeitung entsprechend den Anforderungen der DSGVO enthalten.

Der Verantwortliche kann Subauftragsverarbeiter nach denselben Maßstäben überprüfen wie DID FlexCo selbst (Abschnitt 4.8). DID FlexCo bleibt dem Verantwortlichen gegenüber für die Einhaltung der datenschutzrechtlichen Pflichten ihrer Subauftragsverarbeiter voll verantwortlich.

7. Ort der Verarbeitung und Drittlandübermittlung

Die Datenverarbeitung erfolgt grundsätzlich in der EU bzw. im EWR. Eine Verarbeitung in einem Drittland oder eine Übermittlung an ein Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission (Art. 45 DSGVO) oder geeigneter Garantien wie Standarddatenschutzklauseln (Art. 46 Abs 2 lit c DSGVO).

Die eingesetzten Subauftragsverarbeiter, deren Verarbeitungsorte und die jeweilige Übermittlungsgrundlage ergeben sich aus der Liste der Subauftragsverarbeiter in der jeweils gültigen Fassung (Anhang 3).

8. Haftung

Die Haftung richtet sich nach den gesetzlichen Bestimmungen, den Regelungen des Hauptvertrags sowie der aktuell geltenden Fassung der Allgemeinen Geschäftsbedingungen der DID FlexCo.

DID FlexCo erfüllt die ihr nach dieser Vereinbarung obliegenden Pflichten und haftet für Pflichtverletzungen ihrer Subauftragsverarbeiter nach Maßgabe des Art. 28 Abs 4 DSGVO.

Für leichte Fahrlässigkeit haftet DID FlexCo nur bei Verletzung wesentlicher Vertragspflichten, insbesondere bei Verletzung von Weisungen, der technischen und organisatorischen Maßnahmen sowie der Geheimhaltungs- und Meldepflichten. Die Parteien haften im Übrigen nach den gesetzlichen Bestimmungen. Zwingende gesetzliche Haftungsregelungen, insbesondere Art. 82 DSGVO, bleiben unberührt. Die gesetzlichen Befugnisse der Datenschutzaufsichtsbehörden zur Verhängung von Geldbußen und sonstigen Sanktionen bleiben ebenfalls unberührt.

9. Schlussbestimmungen

DID FlexCo ist berechtigt, diesen Vertrag zu ändern, soweit dies aufgrund gesetzlicher Vorgaben, behördlicher Anordnungen oder technischer bzw. organisatorischer Änderungen erforderlich ist und die Änderungen die Rechte des Verantwortlichen nicht unangemessen beeinträchtigen. Änderungen werden dem Verantwortlichen mindestens sechs Wochen vor ihrem Inkrafttreten in Textform oder über die Plattform mitgeteilt. Widerspricht der Verantwortliche nicht vor dem Inkrafttreten, gelten die Änderungen als vereinbart; auf diese Wirkung wird in der Mitteilung ausdrücklich hingewiesen.

Dieser Vertrag besteht in deutscher und englischer Sprache. Bei Abweichungen geht die englische Fassung vor.

Änderungen und Ergänzungen bedürfen der Textform. Sollte eine Bestimmung dieses Vertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts. Für Streitigkeiten aus diesem Vertrag ist das sachlich zuständige Gericht in Wien zuständig.

Zwingende gesetzliche Bestimmungen über die Rechtswahl und den Gerichtsstand bleiben unberührt.

Anhänge

- Anhang 1 – Gegenstand, Art, Zweck und Dauer der Verarbeitung, Kategorien personenbezogener Daten und betroffener Personen
- Anhang 2 – Technische und organisatorische Maßnahmen
- Anhang 3 – Liste der Subauftragsverarbeiter

Ort, Datum

Verantwortlicher	**DID Daten-Intermediär-Dienste FlexCo**

Anhang 1 – Gegenstand der Verarbeitung

Punkt	Beschreibung
Gegenstand	Bereitstellung neutraler Datenintermediär-Dienste: Entgegennahme, Speicherung und weisungsgemäße Weitergabe der vom Verantwortlichen bereitgestellten Daten sowie Abwicklung der auf der Plattform geschlossenen Vereinbarungen.
Art der Verarbeitung	Erheben, Speichern, Organisieren, Auslesen, Übermitteln, Einschränken und Löschen; Protokollierung der Zugriffe und Vertragsvorgänge.
Zweck	Durchführung der vom Verantwortlichen festgelegten Datenweitergabe und der von ihm beauftragten unterstützenden Leistungen, insbesondere der Speicherung.
Kategorien personenbezogener Daten	Die vom Verantwortlichen bereitgestellten Nutzdaten nach Maßgabe des jeweiligen Datenmodells; Identifikations-, Kontakt- und Vertretungsdaten der handelnden Personen; Anmelde- und Authentifizierungsdaten; Vertrags- und Protokolldaten.
Kategorien betroffener Personen	Personen, deren Daten der Verantwortliche bereitstellt; Vertreterinnen und Vertreter sowie Beschäftigte des Verantwortlichen und der übrigen Vertragsparteien.
Besondere Kategorien	Nicht vorgesehen (Art. 9 DSGVO).
Dauer	Für die Dauer des Hauptvertrags; darüber hinaus nur, soweit gesetzliche Aufbewahrungspflichten bestehen. Die vom Verantwortlichen festgelegte Aufbewahrungsfrist ergibt sich aus der jeweiligen Vereinbarung auf der Plattform der DID FlexCo.

Anhang 2 – Technische und organisatorische Maßnahmen

DID FlexCo setzt die folgenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO um, soweit sie für die konkrete Verarbeitung erforderlich sind.

Vertraulichkeit

Zutrittskontrolle: Alle Produktivsysteme werden in Rechenzentren der in Anhang 3 genannten Dienstleister betrieben; die physische Sicherheit wird über die Lieferantenprüfung, vertragliche Sicherheitspflichten und die Durchsicht der einschlägigen Zertifizierungen sichergestellt.

Zugangskontrolle: Benutzerkonten werden erst nach Identitätsprüfung eingerichtet; für privilegierte Zugänge und Fernzugriffe ist Mehrfaktor-Authentifizierung erforderlich; Sitzungen laufen ab und Konten werden nach wiederholten Fehlversuchen gesperrt; Anmeldevorgänge werden protokolliert.

Zugriffskontrolle: Berechtigungen werden definierten Rollen nach dem Need-to-know-Prinzip zugewiesen, regelmäßig überprüft und bei Rollen- oder Statusänderungen unverzüglich entzogen.

Trennung: Daten verschiedener Verantwortlicher werden getrennt gehalten; Entwicklungs-, Test- und Produktivumgebungen sind organisatorisch und technisch getrennt; das Netzwerk ist segmentiert und folgt einem Default-Deny-Prinzip.

Verschwiegenheit: Alle mit der Verarbeitung befassten Personen sind über das Ende ihrer Tätigkeit hinaus zur Vertraulichkeit verpflichtet und werden regelmäßig zu Datenschutz und Informationssicherheit geschult.

Integrität

Weitergabekontrolle: Daten werden ausschließlich über freigegebene Kanäle und an berechtigte Empfänger übertragen; Verbindungen sind bei der Übertragung verschlüsselt, Daten sind im Ruhezustand verschlüsselt; Übertragungen werden protokolliert.

Eingabekontrolle: Zugriffe und Änderungen werden mit Benutzer, Zeitpunkt, Quelle und Aktion protokolliert; die Zeitquellen sind synchronisiert; Protokolle sind zugriffsgeschützt und gegen Veränderung gesichert.

Änderungsmanagement: Änderungen werden eindeutig erfasst, risikobewertet, freigegeben und sind rücknehmbar; Anfordernde, Freigebende und Umsetzende sind getrennt, soweit umsetzbar; Deployments sind nachvollziehbar.

Berechtigungsverwaltung: Berechtigungen für Zugriff und Offenlegung sind an eine geprüfte Identität und an den konkreten Vertrag und Zweck gebunden, werden bei jeder Offenlegungsanfrage ausgewertet und bei Widerruf unmittelbar durchgesetzt; jede Erteilung, Änderung und jeder Widerruf wird aufgezeichnet.

Verfügbarkeit und Belastbarkeit

Sicherung: Alle kritischen Systeme werden gesichert; Sicherungen werden vor Übertragung und Speicherung verschlüsselt und getrennt von der Produktivumgebung aufbewahrt; der Zugriff darauf ist rollenbasiert und durch Mehrfaktor-Authentifizierung geschützt.

Wiederherstellung: Wiederherstellungs- und Integritätstests erfolgen regelmäßig und nach wesentlichen Änderungen; ein Notfallwiederherstellungsplan wird gepflegt, überprüft und versioniert.

Überwachung: Sicherheitsrelevante Ereignisse werden zentral erfasst, korreliert und alarmiert.

Verfahren zur regelmäßigen Überprüfung

Wirksamkeit: Die Maßnahmen werden regelmäßig überprüft und an den Stand der Technik, die Art der Verarbeitung und die erkennbaren Risiken angepasst.

Auftragskontrolle: Subauftragsverarbeiter werden auf Grundlage einer dokumentierten Risikobewertung ausgewählt, durch einen Auftragsverarbeitungsvertrag mit gleichwertigen Pflichten gebunden und regelmäßig überprüft; die aktuelle Liste ergibt sich aus Anhang 3.

Umgang mit Sicherheitsvorfällen: verpflichtender Meldeweg, zentrale und veränderungssichere Vorfallsaufzeichnungen, festgelegte Reaktions- und Eskalationsverfahren sowie Meldung an den Verantwortlichen nach Abschnitt 4.5.

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen: Datenminimierung, restriktive Voreinstellungen, je Datenkategorie festgelegte und in Produktiv-, Sicherungs- und Protokollsystemen durchgesetzte Aufbewahrungsfristen, Löschung mit Löschnachweis sowie Pseudonymisierung, soweit der Verarbeitungszweck dies zulässt.

DID FlexCo dokumentiert diese Maßnahmen intern im Detail und stellt dem Verantwortlichen auf Anfrage weitere Informationen zur Verfügung.

Anhang 3 – Liste der Subauftragsverarbeiter

Die eingesetzten Subauftragsverarbeiter, deren Namen, ihre erbrachten Leistungen, Verarbeitungsorte sowie gegebenenfalls die Grundlage und Garantien für Drittlandübermittlungen ergeben sich aus der Liste der Subauftragsverarbeiter von DID FlexCo in der jeweils gültigen Fassung. Die Liste ist abrufbar unter:

https://intermediary.at/documents/DID-FlexCo_Sub-Processors.pdf

DID FlexCo hält die Liste aktuell und informiert den Verantwortlichen über Änderungen gemäß Abschnitt 6.

Die Liste ist Bestandteil dieses Vertrags.