

VORLAGE · TOMORIS TOOLBOX

AV-Vertrag: Mustervorlage nach Art. 28 DSGVO mit Prüfliste

Muster mit zwölf Paragraphen und vier Anlagen, belegt mit Art. 28 DSGVO, den EDSA-Leitlinien 07/2020 und dem Durchführungsbeschluss (EU) 2021/915

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/av-vertrag-vorlage

AUF EINEN BLICK

12

Paragraphen Mustertext
mit Platzhaltern

4

Anlagen: Verarbeitung,
TOM, Unterauftrag,
Kontakte

lit. a–h

Pflichtinhalte nach Art. 28
Abs. 3 DSGVO abgedeckt

15

Prüfpunkte für vorgelegte
Verträge

FÜR WEN

- Geschäftsführung und Einkauf, die Dienstleister mit Zugriff auf personenbezogene Daten beauftragen
- Datenschutzverantwortliche und Datenschutzbeauftragte
- IT-Dienstleister, Hosting- und Cloud-Anbieter, die als Auftragsverarbeiter tätig sind
- Rechtsberatung, die einen Ausgangstext für die Verhandlung sucht

WURUM ES GEHT

Wer personenbezogene Daten von einem Dienstleister verarbeiten lässt, braucht nach Art. 28 DSGVO einen Vertrag, der Gegenstand, Weisungen, Sicherheit, Unterauftragsverarbeiter, Unterstützung und Löschung regelt. Dieses Muster setzt die Pflichtinhalte in zwölf Paragraphen mit Platzhaltern um, ergänzt die Empfehlungen des Europäischen Datenschutzausschusses aus den Leitlinien 07/2020 und erklärt, wann die Standardvertragsklauseln der EU-Kommission die bessere Wahl sind. Die Prüfliste hilft, einen vom Dienstleister vorgelegten Vertrag in kurzer Zeit auf Lücken zu prüfen.

Muster von TOMORIS, kein amtlicher Text: Es ist an die konkrete Verarbeitung, den Hauptvertrag und Ihr Unternehmen anzupassen. Es gibt einen Überblick und ersetzt keine Rechtsberatung; maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung.

Nutzung: Diese Vorlage dürfen Sie für den eigenen Gebrauch anpassen; weitergeben dürfen Sie sie nur in unveränderter Form.

INHALT

01	Wann Sie einen AV-Vertrag brauchen	2
02	Pflichtinhalte und wo sie im Muster stehen	3
03	Mustertext, Teil 1: Gegenstand, Weisungen, Sicherheit	4
04	Mustertext, Teil 2: Unterstützung, Prüfungen, Ende	5
05	Anlagen zum Ausfüllen	6
06	Prüfliste für einen vorgelegten AV-Vertrag	7
07	Häufige Fehler	8
08	Quellen	8

01

Wann Sie einen AV-Vertrag brauchen

Rolle des Dienstleisters, Form des Vertrags und die zwei Wege: eigener Vertrag oder Standardvertragsklauseln der EU-Kommission.

Verarbeitet ein Dienstleister personenbezogene Daten im Auftrag und nach Weisung, ist er Auftragsverarbeiter. Der Verantwortliche darf nur mit Auftragsverarbeitern arbeiten, die hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bieten (Art. 28 Abs. 1 DSGVO). Die Verarbeitung erfolgt auf Grundlage eines Vertrags, der schriftlich abzufassen ist, was auch elektronisch erfolgen kann (Abs. 3 und 9). Ob jemand Verantwortlicher oder Auftragsverarbeiter ist, ergibt sich laut Europäischem Datenschutzausschuss (EDSA) aus den tatsächlichen Umständen und ist nicht verhandelbar (Leitlinien 07/2020, Rn. 12). Bestimmt ein Auftragsverarbeiter unter Verstoß gegen die DSGVO selbst Zwecke und Mittel, gilt er insoweit als Verantwortlicher (Art. 28 Abs. 10).

Art. 28 Abs. 6 bis 8 erlaubt einen individuellen Vertrag oder Standardvertragsklauseln, ganz oder teilweise; solche Klauseln legt die Kommission (Abs. 7) oder eine Aufsichtsbehörde (Abs. 8) fest.

Eigener Vertrag

Die Parteien handeln einen Vertrag mit allen Pflichtinhalten aus, etwa auf Basis dieses Musters. Nach dem EDSA soll er die DSGVO nicht nur wiederholen, sondern konkret festlegen, wie die Pflichten erfüllt werden und welches Sicherheitsniveau gilt (Rn. 112).

Standardvertragsklauseln

Die Klauseln im Anhang des Durchführungsbeschlusses (EU) 2021/915 erfüllen Art. 28 Abs. 3 und 4 (Art. 1). Die Parteien verpflichten sich, sie nicht zu ändern, außer zur Ergänzung oder Aktualisierung der Informationen in den Anhängen (Klausel 2 lit. a). Sie dürfen in einen umfangreicheren Vertrag aufgenommen und ergänzt werden, solange nichts im Widerspruch zu ihnen steht (Klausel 2 lit. b).

Dies ist ein Muster von TOMORIS, kein amtlicher Text und nicht identisch mit den Standardvertragsklauseln. Ein Vertrag oder anderes Rechtsinstrument ist Pflicht; ob er auf den Standardvertragsklauseln beruht oder individuell ausgehandelt wird, ist frei. Die Klauseln sind nicht zwingend vorzuziehen (EDSA, Rn. 106). Passen Sie das Muster an die konkrete Verarbeitung an und lassen Sie es bei Bedarf rechtlich prüfen; es ersetzt keine Rechtsberatung.

02

Pflichtinhalte und wo sie im Muster stehen

Was Art. 28 Abs. 3 DSGVO zwingend verlangt, mit dem Paragraphen dieses Musters, der es regelt.

Pflichtinhalte nach Art. 28 Abs. 2 bis 4 DSGVO und ihre Umsetzung im Muster

PFLICHTINHALT	FUNDSTELLE	MUSTER
Gegenstand und Dauer, Art und Zweck, Art der Daten, Kategorien Betroffener, Pflichten und Rechte des Verantwortlichen	Abs. 3 Satz 1	§ 1, § 2, § 9, Anlage 1
Verarbeitung nur auf dokumentierte Weisung, auch für Drittlandübermittlungen; Hinweis bei datenschutzwidriger Weisung	Abs. 3 lit. a, Unterabs. 2	§ 2, § 8
Vertraulichkeit der befugten Personen	Abs. 3 lit. b	§ 3
Alle nach Art. 32 erforderlichen Maßnahmen	Abs. 3 lit. c	§ 4, Anlage 2
Bedingungen für Unterauftragsverarbeiter: Genehmigung, Information, Einspruch, gleiche Pflichten	Abs. 2, Abs. 3 lit. d, Abs. 4	§ 5, Anlage 3
Unterstützung bei Anträgen Betroffener	Abs. 3 lit. e	§ 6
Unterstützung bei Sicherheit, Meldung von Verletzungen, Folgenabschätzung, Konsultation (Art. 32 bis 36)	Abs. 3 lit. f	§ 7
Löschen oder Rückgabe nach Wahl des Verantwortlichen, Löschung vorhandener Kopien	Abs. 3 lit. g	§ 10

03 —

Mustertext, Teil 1: Gegenstand, Weisungen, Sicherheit

§ 1 bis § 5 zum Übernehmen und Anpassen; eckige Klammern sind Platzhalter oder Auswahl.

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO zwischen [Name, Anschrift] als Verantwortlichem und [Name, Anschrift] als Auftragsverarbeiter, im Folgenden die Parteien.

§ 1 Gegenstand und Dauer. (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen von [Hauptvertrag, Datum]. Gegenstand, Art und Zweck der Verarbeitung, Art der Daten, Kategorien betroffener Personen und Orte der Verarbeitung ergeben sich aus Anlage 1. (2) Der Vertrag gilt ab [Datum] für die Dauer des Hauptvertrags [oder: bis Datum]; Pflichten aus § 10 gelten darüber hinaus bis zu ihrer Erfüllung. (3) Der Verantwortliche stellt die Daten bereit, erteilt und dokumentiert Weisungen (§ 2) und überwacht die Verarbeitung, auch durch Prüfungen (§ 9).

§ 2 Weisungen. (1) Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen an ein Drittland oder eine internationale Organisation, sofern er nicht nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, soweit das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. (2) Weisungen erteilen die in Anlage 4 genannten Personen in Textform; die Parteien bewahren sie mit diesem Vertrag auf. (3) Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, informiert er den Verantwortlichen unverzüglich und darf ihre Ausführung bis zur Bestätigung, Änderung oder Rücknahme aussetzen.

§ 3 Vertraulichkeit. Der Auftragsverarbeiter gewährt Zugang zu den Daten nur Personen, die ihn für ihre Aufgaben benötigen, und stellt sicher, dass sie zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 4 Sicherheit der Verarbeitung. (1) Der Auftragsverarbeiter ergreift alle nach Art. 32 DSGVO erforderlichen Maßnahmen, mindestens die in Anlage 2 konkret beschriebenen. (2) Er überprüft sie regelmäßig, mindestens [jährlich], auf ihre Angemessenheit. (3) Änderungen, die das Schutzniveau senken könnten, bedürfen der vorherigen Zustimmung des Verantwortlichen in Textform; andere Änderungen teilt er [innerhalb von Frist] mit.

§ 5 Unterauftragsverarbeiter. (1) Zutreffende Option wählen. Option A, gesonderte Genehmigung: Der Auftragsverarbeiter setzt weitere Auftragsverarbeiter nur mit vorheriger gesonderter Genehmigung des Verantwortlichen in Textform ein und beantragt sie mindestens [Frist] vorher. Option B, allgemeine Genehmigung: Der Verantwortliche genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter. Über jede beabsichtigte Hinzuziehung oder Ersetzung informiert der Auftragsverarbeiter mindestens [Frist] vorher in Textform; der Verantwortliche kann innerhalb von [Frist] Einspruch erheben, Folge: [Regelung]. (2) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf wie in diesem Vertrag und haftet gegenüber dem Verantwortlichen für deren Einhaltung (Art. 28 Abs. 4 DSGVO).

04 —

Mustertext, Teil 2: Unterstützung, Prüfungen, Ende

§ 6 bis § 12: Betroffenenrechte, Datenpannen, Drittländer, Nachweise, Löschung, Verstöße und Schlussbestimmungen.

§ 6 Rechte betroffener Personen. Der Auftragsverarbeiter leitet Anträge betroffener Personen unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst, es sei denn, der Verantwortliche ermächtigt ihn dazu. Er unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung, etwa durch [Export, Berichtigung, Löschung im System].

§ 7 Unterstützung bei Pflichten nach Art. 32 bis 36 DSGVO. (1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens [Anzahl] Stunden nach Kenntnis, an [Kontakt aus Anlage 4], mit den ihm bekannten Angaben nach Art. 33 Abs. 3 DSGVO; fehlende Angaben liefert er nach, sobald sie vorliegen. (2) Er unterstützt den Verantwortlichen bei Sicherheitsmaßnahmen, Meldungen an Aufsichtsbehörde und Betroffene, Datenschutz-Folgenabschätzungen und vorheriger Konsultation, unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen.

§ 8 Orte der Verarbeitung und Drittländer. Die Verarbeitung erfolgt an den in Anlage 1 genannten Orten. Übermittlungen an ein Drittland oder eine internationale Organisation, auch durch Unterauftragsverarbeiter oder Fernzugriff, erfolgen nur auf dokumentierte Weisung und nur, wenn die Bedingungen von Kapitel V DSGVO erfüllt sind; Grundlage: [Angemessenheitsbeschluss nach Art. 45, Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DSGVO (Durchführungsbeschluss (EU) 2021/914)].

§ 9 Nachweise und Prüfungen. (1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags und des Art. 28 DSGVO erforderlich sind. (2) Er ermöglicht Überprüfungen und Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer und trägt dazu bei; Inspektionen vor Ort werden mit [Frist] Vorankündigung durchgeführt. Zertifizierungen und Prüfberichte des Auftragsverarbeiters kann der Verantwortliche berücksichtigen; die Auswahl des Prüfers trifft der Verantwortliche. (3) Kosten: [Regelung].

§ 10 Löschung und Rückgabe. Nach Ende der Leistung löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten und bestätigt dies in Textform, oder er gibt sie in [Format] zurück und löscht vorhandene Kopien, sofern nicht Unionsrecht oder das Recht eines Mitgliedstaats eine Speicherung verlangt. Die Wahl trifft der Verantwortliche [im Vertrag: Löschung oder Rückgabe] und kann sie bis zum Ende der Leistung ändern. Bis zur Löschung gilt dieser Vertrag fort.

§ 11 Verstöße und Beendigung. Kann der Auftragsverarbeiter diesen Vertrag nicht einhalten, informiert er den Verantwortlichen unverzüglich. Der Verantwortliche kann die Verarbeitung dann aussetzen lassen und den Vertrag, soweit er die Auftragsverarbeitung betrifft, kündigen, wenn die Einhaltung nicht innerhalb von [Frist] wiederhergestellt ist.

§ 12 Schlussbestimmungen. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag geht dieser Vertrag in Fragen des Datenschutzes vor. Änderungen bedürfen der Textform. Textform im Sinne dieses Vertrags ist eine dauerhaft speicherbare Erklärung, die den Erklärenden erkennen lässt, etwa eine E-Mail (elektronisches Format nach Art. 28 Abs. 9 DSGVO). Die Haftung richtet sich nach [Hauptvertrag]; Art. 82 DSGVO bleibt unberührt. Anlagen 1 bis 4 sind Bestandteil des Vertrags. Ort, Datum, Unterschriften beider Parteien.

05

Anlagen zum Ausfüllen

Beschreibung der Verarbeitung, technische und organisatorische Maßnahmen, Unterauftragsverarbeiter und Kontakte.

Anlage 1: Beschreibung der Verarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

ANGABE	EINTRAG
Gegenstand: Hauptgegenstand der Verarbeitung, präzise genug, dass Dritte ihn verstehen	_____
Art und Zweck der Verarbeitung: Vorgänge wie Speichern, Sichern, Fernwartung, Versand, und wofür	_____
Art der personenbezogenen Daten, besondere Kategorien konkret benennen	_____
Kategorien betroffener Personen, z. B. Beschäftigte, Kundinnen und Kunden, Besucher	_____
Dauer der Verarbeitung oder Kriterien dafür	_____
Orte der Verarbeitung, auch Fernzugriff und Support	_____

Anlage 2: Technische und organisatorische Maßnahmen, konkret statt allgemein beschrieben

BEREICH NACH ART. 32 ABS. 1 DSGVO	MASSNAHMEN DES AUF- TRAGSVERARBEITERS
a) Pseudonymisierung und Verschlüsselung	_____
b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste	_____
c) Rasche Wiederherstellung nach einem Zwischenfall	_____
d) Regelmäßige Überprüfung und Bewertung der Wirksamkeit	_____

Anlage 3: Genehmigte Unterauftragsverarbeiter

NAME, ANSCHRIFT	LEISTUNG	ORT, BEI DRITTLAND GRUNDLAGE
_____	_____	_____
_____	_____	_____

Anlage 4: Weisungsberechtigte und Kontakte

ROLLE	VERANTWORTLICHER	AUFTRAGSVERARBEITER
Weisungsberechtigt bzw. Weisungsempfänger	_____	_____
Meldungen von Datenschutzverletzungen	_____	_____
Datenschutzbeauftragter, falls bestellt	_____	_____

06 —

Prüfliste für einen vorgelegten AV-Vertrag

Viele Dienstleister legen eigene Verträge vor; diese Punkte zeigen in kurzer Zeit, ob etwas fehlt.

- ☐ Rollen stimmen mit der Wirklichkeit überein: Der Dienstleister entscheidet nicht selbst über Zwecke, etwa eigene Analysen oder Training mit Ihren Daten
- ☐ Gegenstand, Art, Zweck, Datenarten und Betroffene sind konkret beschrieben, nicht nur „personenbezogene Daten nach Art. 4“ (EDSA, Rn. 114)
- ☐ Verarbeitung nur auf dokumentierte Weisung; geregelt ist, wer Weisungen erteilt und wie sie dokumentiert werden
- ☐ Hinweispflicht bei datenschutzwidrigen Weisungen und Folge, etwa Aussetzen (EDSA, Rn. 149)
- ☐ Vertraulichkeitsverpflichtung der Beschäftigten des Dienstleisters
- ☐ TOM konkret beschrieben oder als aktuelles Dokument beigelegt; Änderungen nicht zulasten des Schutzniveaus
- ☐ Unterauftragsverarbeiter: Liste vorhanden, gesonderte oder allgemeine Genehmigung, Ankündigungsfrist, Einspruchsrecht und dessen Folge, gleiche Pflichten und Haftung des Dienstleisters für sie
- ☐ Orte der Verarbeitung genannt, Drittlandübermittlungen nur mit Grundlage nach Kapitel V
- ☐ Unterstützung bei Betroffenenrechten, ohne dass der Dienstleister Anträge selbst beantwortet
- ☐ Meldung von Datenschutzverletzungen unverzüglich, mit Frist in Stunden, Kontaktstelle und Mindestangaben (EDSA, Rn. 136)
- ☐ Unterstützung bei Folgenabschätzung und Konsultation
- ☐ Nachweise und Prüfrecht für Sie oder einen von Ihnen beauftragten Prüfer, nicht nur Zertifikate nach Wahl des Dienstleisters
- ☐ Löschen oder Rückgabe nach Ihrer Wahl, Löschung vorhandener Kopien, mit Bestätigung und Frist
- ☐ Vorrang des AV-Vertrags vor allgemeinen Geschäftsbedingungen in Datenschutzfragen
- ☐ Schriftlich oder elektronisch abgeschlossen und abgelegt, Verweis im Verarbeitungsverzeichnis

07 —

Häufige Fehler

Was AV-Verträge in der Praxis schwächt und wie Sie es vermeiden.

- Vertrag wiederholt nur Art. 28: Ohne konkrete Weisungen, Fristen und Maßnahmen lässt sich im Ernstfall nichts nachweisen (EDSA, Rn. 112).
- Standardvertragsklauseln umformuliert: Wer ihren Text ändert, nutzt nicht mehr die Klauseln, deren Eignung der Beschluss feststellt (Art. 1); ergänzen dürfen Sie nur die Anhänge und widerspruchsfreie Zusatzklauseln (Klausel 2).
- Liste der Unterauftragsverarbeiter fehlt oder ist veraltet; Änderungen werden nur auf einer Website veröffentlicht, ohne dass Sie Einspruch erheben können.
- Rolle falsch eingeordnet: Nicht jeder Dienstleister ist Auftragsverarbeiter. Wer über Zwecke und wesentliche Mittel selbst entscheidet, ist Verantwortlicher (EDSA, Rn. 39 f.); dann passt kein AV-Vertrag, sondern etwa eine Vereinbarung nach Art. 26 DSGVO bei gemeinsamer Verantwortlichkeit.
- Vertrag abgeschlossen, aber nie gelebt: Weisungen nicht dokumentiert, Prüfungen nie durchgeführt, Löschung am Ende nicht bestätigt.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **Verordnung (EU) 2016/679 (DSGVO), berichtigt ABl. L 127 vom 23.5.2018**
Art. 26, 28, 29, 32, 33 Abs. 3, 45, 46, 82 und Kapitel V; Art. 28 Abs. 3 lit. g in der berichtigten Fassung
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 2 **Durchführungsbeschluss (EU) 2021/915: Standardvertragsklauseln nach Art. 28 Abs. 7 DSGVO**
Art. 1 und 2, Erwägungsgründe 5 und 6, Klauseln 2, 7, 8, 9 und 10, Anhänge I bis IV
eur-lex.europa.eu/eli/dec_impl/2021/915/oj/deu
- 3 **Durchführungsbeschluss (EU) 2021/914: Standardvertragsklauseln für Drittländer**
Art. 1 Abs. 1: Garantien nach Art. 46 Abs. 2 lit. c DSGVO
eur-lex.europa.eu/eli/dec_impl/2021/914/oj/deu
- 4 **EDSA-Leitlinien 07/2020 zu Verantwortlichem und Auftragsverarbeiter**
Version 2.0 vom 7.7.2021, Rn. 12, 39 f., 104 bis 159
www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_...
- 5 **Vorschlag Digital-Omnibus COM(2025) 837, Verfahren 2025/0360(COD)**
geprüft: keine Änderung von Art. 28 DSGVO vorgeschlagen; Stand 25.10.2026 im Verfahren
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837