

Formenio

Auftragsverarbeitungsvertrag

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Stand: April 2026

zwischen

dem Nutzer der Formenio-Plattform (nachfolgend „Auftraggeber“ oder „Verantwortlicher“)

und

David Walter

Formenio.de

Mainzer Str. 40

67657 Kaiserslautern

E-Mail: hallo@formenio.de

(nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“)

– gemeinsam „die Parteien“ –

Präambel

Der Auftraggeber nutzt die SaaS-Plattform Formenio des Auftragnehmers, um Online-Formulare zu erstellen und zu veröffentlichen. Im Rahmen dieser Nutzung werden über die Formulare des Auftraggebers personenbezogene Daten von dessen Endnutzern erhoben und auf Servern des Auftragnehmers gespeichert und verarbeitet.

Der Auftraggeber ist insoweit Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO; der Auftragnehmer ist Auftragsverarbeiter im Sinne von Art. 4 Nr. 8, Art. 28 DSGVO. Dieser Vertrag regelt die datenschutzrechtlichen Anforderungen an die Auftragsverarbeitung gemäß Art. 28 DSGVO.

Dieser AVV wird durch die Akzeptanz der AGB von Formenio und die Nutzung der Plattform zur Verarbeitung personenbezogener Daten Dritter zwischen den Parteien wirksam geschlossen. Er gilt in der jeweils auf <https://formenio.de/avv> veröffentlichten Fassung.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Auftragsverarbeitung ist die Speicherung und Verarbeitung personenbezogener Daten, die über die vom Auftraggeber auf der Formenio-Plattform erstellten Formulare erhoben werden, gemäß Anlage 1 dieses Vertrages.

(2) Die Verarbeitung erfolgt für die Dauer des Nutzungsvertrages (AGB) zwischen den Parteien. Nach Beendigung des Nutzungsvertrages gilt § 10 dieses AVV.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer sind in Anlage 1 im Einzelnen festgelegt.

(2) Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und nicht für eigene Zwecke, soweit nicht das Unionsrecht oder das Recht der Mitgliedstaaten eine Verarbeitung vorschreibt. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der

Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(3) Die Nutzung der Plattform gemäß deren bestimmungsgemäßem Zweck gilt als dokumentierte Weisung des Auftraggebers.

§ 3 Weisungsrecht des Auftraggebers

(1) Der Auftraggeber ist gegenüber dem Auftragnehmer weisungsbefugt hinsichtlich der Verarbeitung personenbezogener Daten. Weisungen können schriftlich oder in Textform (z. B. per E-Mail an hallo@formenio.de) erteilt werden.

(2) Hält der Auftragnehmer eine Weisung des Auftraggebers für datenschutzrechtlich unzulässig, ist er berechtigt, die Ausführung der betreffenden Weisung bis zu einer Klärung durch den Auftraggeber auszusetzen. Er hat den Auftraggeber unverzüglich über seine Bedenken zu informieren.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer gewährleistet, dass alle zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) Der Auftragnehmer stellt sicher, dass der Zugang zu den verarbeiteten Daten auf das für die Leistungserbringung erforderliche Minimum beschränkt ist (Need-to-know-Prinzip).

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO, insbesondere die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen (TOMs), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die TOMs können vom Auftragnehmer im Laufe der Zeit angepasst und verbessert werden, sofern das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer informiert den Auftraggeber über wesentliche Änderungen.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, die in Anlage 3 genannten Unterauftragsverarbeiter einzusetzen.

(2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder den Austausch von Unterauftragsverarbeitern mit einer Vorlaufzeit von mindestens 14 Tagen (z. B. über die Aktualisierung dieser Seite und/oder per E-Mail).

Widerspricht der Auftraggeber nicht fristgerecht, gilt die Änderung als genehmigt. Im Falle eines begründeten Widerspruchs sind die Parteien berechtigt, den Vertrag mit einer Frist von 30 Tagen zu kündigen.

(3) Der Auftragnehmer stellt durch entsprechende vertragliche Regelungen sicher, dass Unterauftragsverarbeiter vergleichbaren datenschutzrechtlichen Verpflichtungen unterliegen wie der Auftragnehmer im Verhältnis zum Auftraggeber.

§ 7 Unterstützung bei der Wahrnehmung von Betroffenenrechten

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit und soweit technisch realisierbar bei der Erfüllung seiner Pflichten gegenüber betroffenen Personen (Art. 12–22

DSGVO), insbesondere bei Auskunfts-, Berichtigungs-, Löschungs- und Einschränkungsanfragen.

(2) Wenden sich betroffene Personen direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter, ohne selbst inhaltlich zu antworten.

(3) Der Auftragnehmer stellt dem Auftraggeber die hierfür erforderlichen Daten-Exportfunktionen über das Nutzerkonto bereit.

§ 8 Unterstützung bei weiteren datenschutzrechtlichen Pflichten

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung folgender Pflichten:

- der Sicherheitspflicht nach Art. 32 DSGVO,
- der Meldepflicht bei Datenschutzverletzungen nach Art. 33 f. DSGVO,
- der Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 f. DSGVO, soweit erforderlich.

§ 9 Datenschutzverletzungen

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, in der Regel innerhalb von 24 Stunden nach Bekanntwerden, über Verletzungen des Schutzes personenbezogener Daten des Auftraggebers.

(2) Die Meldung enthält mindestens:

- eine Beschreibung der Art der Verletzung (soweit möglich),
- die Kategorien und die geschätzte Anzahl der betroffenen Personen und Datensätze,
- die voraussichtlichen Folgen der Verletzung sowie
- die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung.

(3) Eine verzögerte Meldung über 72 Stunden nach Bekanntwerden muss gegenüber der zuständigen Aufsichtsbehörde begründet werden; der Auftragnehmer wird den Auftraggeber so früh wie möglich informieren, um ihm eine fristgerechte Meldung zu ermöglichen.

§ 10 Löschung und Rückgabe von Daten nach Vertragsende

(1) Nach Beendigung des Nutzungsvertrages stellt der Auftragnehmer dem Auftraggeber sämtliche personenbezogenen Daten für einen Zeitraum von 30 Tagen zum Export bereit.

(2) Nach Ablauf dieser Exportfrist löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen, die eine weitere Speicherung erfordern.

(3) Auf schriftliche Anforderung bestätigt der Auftragnehmer die erfolgte Löschung.

§ 11 Nachweise, Kontrollen und Audits

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(2) Der Auftragnehmer ermöglicht dem Auftraggeber oder einem von ihm beauftragten, zur Vertraulichkeit verpflichteten Prüfer Überprüfungen und trägt zu diesen bei. Derartige Prüfungen sind dem Auftragnehmer mindestens 4 Wochen im Voraus anzukündigen, auf das notwendige Maß zu beschränken und so durchzuführen, dass der Geschäftsbetrieb des Auftragnehmers nicht übermäßig beeinträchtigt wird.

(3) Als gleichwertige Maßnahme kann der Auftragnehmer einschlägige Zertifizierungen oder Prüfberichte akkreditierter Stellen vorlegen.

§ 12 Haftung

(1) Die Haftung der Parteien in Fällen einer Verletzung dieser Vereinbarung bestimmt sich nach den Vorschriften der DSGVO sowie nach dem Nutzungsvertrag (AGB).

(2) Der Auftraggeber ist als Verantwortlicher allein dafür verantwortlich, dass für die Erhebung und Verarbeitung der personenbezogenen Daten über seine Formulare eine geeignete Rechtsgrundlage nach der DSGVO vorliegt und die betroffenen Personen in geeigneter Weise informiert werden.

§ 13 Geltungsbereich und Rangfolge

Dieser AVV ergänzt den Nutzungsvertrag (AGB) zwischen den Parteien. Bei Widersprüchen zwischen diesem AVV und dem Nutzungsvertrag hat dieser AVV im Hinblick auf datenschutzrechtliche Fragen Vorrang. Im Übrigen gilt deutsches Recht.

Anlage 1: Beschreibung der Auftragsverarbeitung

1. Kategorien betroffener Personen

Endnutzer der Online-Formulare des Auftraggebers, insbesondere: Kunden, Interessenten, Bewerber, Mitarbeiter oder sonstige natürliche Personen, denen der Auftraggeber seine Formulare zur Verfügung stellt.

2. Kategorien personenbezogener Daten

Die vom Auftraggeber in seinen Formularen definierten Datenfelder; typischerweise umfasst dies: Name, Kontaktdaten (E-Mail-Adresse, Telefonnummer, Postanschrift), freitextbasierte Antworten sowie weitere vom Auftraggeber individuell gewählte Felder.

Hinweis: Die Erhebung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO (z. B. Gesundheitsdaten, politische Meinungen, religiöse Überzeugungen) ist nur zulässig, wenn der Auftraggeber über eine geeignete Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO verfügt und die Nutzungsbedingungen des Anbieters einhält.

3. Zweck der Verarbeitung

- Technische Bereitstellung der Formenio-Plattform für den Auftraggeber,
- Entgegennahme, Speicherung und Übermittlung von Formularantworten an den Auftraggeber,
- Bereitstellung von Export- und Auswertungsfunktionen für den Auftraggeber.

4. Art der Verarbeitung

Erhebung, Speicherung, strukturierte Darstellung, Übermittlung und Löschung von Formularantworten entsprechend den Weisungen des Auftraggebers.

5. Ort der Verarbeitung

Europäische Union / Europäischer Wirtschaftsraum (Backend-Server: 1&1 IONOS SE, Deutschland). Die Website wird zusätzlich über Amazon Web Services EMEA SARL (Luxemburg) bereitgestellt.

Anlage 2: Technische und organisatorische Maßnahmen (TOMs)

Die nachfolgenden TOMs werden durch den Auftragnehmer implementiert und regelmäßig überprüft:

1. Zutrittskontrolle

Physischer Schutz der Server durch den zertifizierten Hosting-Anbieter IONOS mit Zugangskontrolle zu Rechenzentren (Sicherheitsschleusen, Videoüberwachung, Schutzmechanismen gegen unbefugten Zutritt).

2. Zugangskontrolle

Passwortgeschützte Nutzerkonten; Empfehlung der Nutzung sicherer Passwörter; automatischer Sitzungsablauf nach Inaktivität.

3. Zugriffskontrolle

Rollenbasierte Zugriffskontrolle: Jeder Nutzer sieht ausschließlich die Daten seines eigenen Kontos (Mandantentrennung). Zugriff der Mitarbeiter des Auftragnehmers auf Kundendaten nur nach dem Need-to-know-Prinzip und nur zur Wartung und zum Support.

4. Weitergabekontrolle

Verschlüsselung aller Datenübertragungen mittels TLS/SSL (HTTPS); keine unverschlüsselte Übertragung von personenbezogenen Daten.

5. Eingabekontrolle

Protokollierung von Systemzugriffen und wesentlichen Systemereignissen zur Nachvollziehbarkeit von Dateneingaben und -änderungen.

6. Verfügbarkeitskontrolle

Regelmäßige Datensicherungen durch den Hosting-Anbieter IONOS; redundante Systemarchitektur zur Minimierung von Ausfallzeiten.

7. Trennungskontrolle

Logische Trennung der Daten verschiedener Auftraggeber in der Datenbankarchitektur; keine übergreifende Auswertung von Kundendaten.

8. Verfahren zur regelmäßigen Überprüfung

Regelmäßige interne Überprüfung der Wirksamkeit der TOMs; Aktualisierung bei Änderung der Verarbeitungstätigkeiten oder des Risikoprofils.

Anlage 3: Unterauftragsverarbeiter

Der Auftragnehmer setzt folgende Unterauftragsverarbeiter ein:

Unternehmen	Sitz	Zweck	Drittlandtransfer
1&1 IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	Backend-Hosting, Datenspeicherung, Webanalyse	Nein (EU/EWR)
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, 1855 Luxemburg	Website-Hosting (Frontend)	Ggf. in die USA; Standardvertragsklauseln (SCCs) + EU-US DPF
Cloudflare Inc.	101 Townsend St., San Francisco, CA 94107, USA	Bot-Schutz / Sicherheit (Turnstile)	USA; Standardvertragsklauseln (SCCs) + EU-US DPF zertifiziert

Hinweis: Änderungen an der Liste der Unterauftragsverarbeiter werden gemäß § 6 Abs. 2 dieses AVV bekannt gegeben. Die jeweils aktuelle Liste ist unter <https://formenio.de/avv> abrufbar.

Dieser AVV gilt als abgeschlossen, wenn der Auftraggeber (Nutzer) die AGB von Formenio akzeptiert und über seine Formulare personenbezogene Daten verarbeitet.