GEMÄSS ART. 28 ABS. 3 DSGVO

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

HINWEIS

> **Musterfassung.** Dieses Dokument zeigt den Vertragstext ohne Kundendaten. Die für Ihr Konto verbindliche Fassung finden Sie angemeldet unter „Einstellungen → Auftragsverarbeitung“.

MUSTER

PARTEIEN

Verantwortlicher (nachfolgend „Kunde“)	[Firma des Kunden] [Straße und Hausnummer] [PLZ und Ort] [Land] vertreten durch [vertretungsberechtigte Person]
Auftragsverarbeiter (nachfolgend „Anbieter“)	Daniel Proschko Bahnhofstr. 8 82216 Maisach Deutschland E-Mail: support@formdall.de Telefon: +49 8141 5098849 USt-IdNr. DE296989995

Formdall ist die Produktbezeichnung des vom Anbieter als Einzelunternehmer betriebenen Dienstes; Vertragspartner ist die vorgenannte natürliche Person.

MUSTER

PRÄAMBEL

Präambel

(1) Der Kunde nutzt Formdall, um Einsendungen aus HTML-Formularen auf seinen eigenen Websites entgegenzunehmen, zu speichern, anzuzeigen und an von ihm bestimmte Ziele weiterzuleiten. Der Anbieter verarbeitet die dabei anfallenden personenbezogenen Daten der Einsender ausschließlich im Auftrag und nach Weisung des Kunden.

(2) Der Kunde ist für diese Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO, der Anbieter Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO. Dieser Vertrag konkretisiert die Pflichten beider Parteien nach Art. 28 DSGVO und ist Bestandteil des zwischen ihnen bestehenden Nutzungsvertrags.

(3) Nicht Gegenstand dieses Vertrags sind Verarbeitungen, für die der Anbieter selbst Verantwortlicher ist. Dazu zählen insbesondere die Verwaltung des Kundenkontos und der Zugangsdaten des Kunden, die Abrechnung kostenpflichtiger Pläne, der Versand von System-E-Mails an den Kunden sowie der Betrieb der Website formdall.de. Über diese Verarbeitungen informiert die Datenschutzerklärung des Anbieters.

§ 1 Gegenstand, Dauer und Beendigung

GEGENSTAND UND DAUER

(1) Gegenstand dieses Vertrags ist die Verarbeitung von Formulareinsendungen im Auftrag des Kunden im Rahmen der Erbringung des Dienstes Formdall nach Maßgabe des Nutzungsvertrags und der Allgemeinen Geschäftsbedingungen des Anbieters (nachfolgend „AGB“).

(2) Der Gegenstand der Verarbeitung ergibt sich im Einzelnen aus § 2 dieses Vertrags sowie aus der Konfiguration, die der Kunde in seinem Konto vornimmt.

(3) Dieser Vertrag beginnt mit dem Nutzungsvertrag und läuft für dessen Dauer. Er endet automatisch mit dem Ende des

MUSTER

Nutzungsvertrags, ohne dass es einer gesonderten Kündigung bedarf. Eine isolierte Kündigung allein dieses Vertrags ist nicht möglich, weil die Verarbeitung im Auftrag mit der Erbringung des Dienstes untrennbar verbunden ist.

(4) Bestimmungen, die ihrem Sinn nach über das Vertragsende hinaus gelten sollen — insbesondere § 4 (Vertraulichkeit), § 9 (Löschung und Rückgabe) und § 10 (Nachweise und Überprüfungen) — bleiben nach Beendigung wirksam, bis sie erfüllt sind.

§ 2

ART, ZWECK, DATENARTEN

Art und Zweck der Verarbeitung, Datenarten, Kategorien betroffener Personen

(1) **Art der Verarbeitung.** Der Anbieter erhebt die Einsendung über seine Schnittstelle, prüft und filtert sie zur Abwehr von Spam und automatisierten Angriffen, speichert sie, ordnet sie dem Formular des Kunden zu, hält sie zum Auslesen und zur Anzeige im Posteingang bereit, ermöglicht ihren Export, übermittelt sie an die vom Kunden konfigurierten Ziele und löscht sie nach Ablauf der vom Kunden festgelegten Aufbewahrungsdauer.

(2) **Zweck der Verarbeitung.** Die Verarbeitung dient allein der Erbringung des Dienstes für den Kunden. Der Anbieter verarbeitet die im Auftrag verarbeiteten Daten nicht zu eigenen Zwecken, insbesondere nicht zu Werbe- oder Profilbildungszwecken und nicht zum Training von Systemen künstlicher Intelligenz. Eine Auswertung der

MUSTER

Einsendungsinhalte findet nicht statt; für Betriebsstatistiken verwendet der Anbieter ausschließlich inhaltsfreie Zählwerte (Anzahl der Einsendungen je Formular und Zeitraum, Anzahl und Grund abgewiesener Einsendungen).

(3) **Datenarten.** Verarbeitet werden sämtliche Felder, die der Kunde in seinem Formular erhebt und deren Inhalt er durch die Gestaltung des Formulars bestimmt; typischerweise sind dies Name, E-Mail-Adresse, Betreff und eine Freitextnachricht. Hinzu treten technische Metadaten der Einsendung: der Hashwert der IP-Adresse des Einsenders, der Ursprungs-Host des absendenden Formulars, der Zeitpunkt des Eingangs sowie Zeitpunkt, Ziel und Ergebnis von Zustellversuchen an die vom Kunden konfigurierten Ziele.

(4) **Umfang in der Hand des Kunden.** Welche Datenarten im Einzelnen anfallen, bestimmt allein der Kunde. Der Kunde erhebt über seine Formulare keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO und keine Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO, es sei denn, die Parteien vereinbaren dies gesondert in Textform. Der Dienst nimmt keine Dateianhänge entgegen und speichert keine hochgeladenen Dateien.

(5) **Kategorien betroffener Personen.** Betroffen sind die natürlichen Personen, die Formulare des Kunden ausfüllen und absenden (nachfolgend „Einsender“), sowie diejenigen Personen, deren Daten ein

MUSTER

Einsender in einem Formularfeld angibt.

(6) **Ort der Verarbeitung.** Die Verarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt. Eine Verarbeitung in einem Drittland außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums findet nicht statt; § 6 Abs. 6 (vom Kunden eingerichtete Zieldienste) bleibt unberührt.

§ 3

WEISUNGSRECHT

Weisungsrecht des Verantwortlichen und Hinweispflicht bei rechtswidrigen Weisungen

(1) Der Anbieter verarbeitet die im Auftrag verarbeiteten Daten ausschließlich auf dokumentierte Weisung des Kunden, auch in Bezug auf eine Übermittlung an ein Drittland (Art. 28 Abs. 3 lit. a DSGVO). Etwas anderes gilt nur, wenn der Anbieter nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Kunden die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Ursprüngliche Weisung sind dieser Vertrag einschließlich seiner Anlagen sowie der Nutzungsvertrag. Als dokumentierte Weisung gilt darüber hinaus die Konfiguration, die der Kunde in seinem Konto vornimmt. Dazu zählen insbesondere:

- die Anlage von Formularen sowie die Bezeichnung, Anzahl und Art der erhobenen Felder einschließlich eines vom Kunden festgelegten

MUSTER

Feldschemas,

- die Entscheidung, ob Einsendungen überhaupt gespeichert werden, und die je Formular festgelegte Aufbewahrungsdauer,
- die Einstellungen zur Spam- und Missbrauchsabwehr, einschließlich der Wahl des Captcha-Verfahrens,
- E-Mail-Benachrichtigungen und automatische Antworten an den Einsender einschließlich der hinterlegten Empfängeradressen,
- Webhooks sowie eingerichtete Connectoren zu Zieldiensten des Kunden einschließlich der Auswahl der zu übermittelnden Felder,
- die Vergabe von Zugriffsrechten an Mitglieder des Arbeitsbereichs sowie die Ausführung von Export- und Löschfunktionen.

(3) Der Kunde kann seine Konfiguration jederzeit im Konto ändern. Jede Änderung ist eine geänderte Weisung und wird ab dem Zeitpunkt ihrer Speicherung befolgt. Bereits abgeschlossene Verarbeitungsvorgänge, insbesondere bereits an ein vom Kunden bestimmtes Ziel übermittelte Einsendungen, bleiben davon unberührt.

(4) Weisungen außerhalb des Kontos erteilt der Kunde in Textform an support@formdall.de. Der Anbieter dokumentiert solche Weisungen und ihre Ausführung. Mündliche Weisungen bestätigt der Kunde unverzüglich in Textform.

(5) Weisungsbefugt auf Seiten des Kunden sind die Personen, denen der Kunde in seinem Konto eine entsprechende Rolle zugewiesen hat, sowie

MUSTER

Personen, die der Kunde dem Anbieter gegenüber in Textform benennt. Für die Aktualität dieser Zuweisungen ist der Kunde verantwortlich; der Anbieter darf auf die im Konto hinterlegten Rollen vertrauen.

(6) Ist der Anbieter der Auffassung, dass eine Weisung des Kunden gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, informiert er den Kunden unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Der Anbieter ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis der Kunde sie bestätigt oder ändert. Bestätigt der Kunde eine Weisung, deren Rechtswidrigkeit für den Anbieter offensichtlich ist, darf der Anbieter ihre Ausführung dauerhaft verweigern.

(7) Der Kunde ist dafür verantwortlich, dass er für die von ihm veranlasste Verarbeitung über eine Rechtsgrundlage verfügt und seine Einsender nach Art. 13 und 14 DSGVO informiert. Der Anbieter schuldet keine Prüfung der Zulässigkeit der Erhebung durch den Kunden.

§ 4 Vertraulichkeit der zur Verarbeitung befugten Personen

VERTRAULICHKEIT

(1) Der Anbieter ist eine natürliche Person und erbringt die Leistung im Wesentlichen persönlich. Er ist zur Vertraulichkeit hinsichtlich der im Auftrag verarbeiteten Daten verpflichtet. Die Verpflichtung besteht auch nach Beendigung dieses Vertrags fort.

(2) Setzt der Anbieter Beschäftigte oder sonstige Personen ein, die Zugang zu den im Auftrag verarbeiteten Daten erhalten können,

MUSTER

verpflichtet er diese vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit, soweit sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO), und macht sie mit den für ihre Tätigkeit maßgeblichen Bestimmungen des Datenschutzrechts vertraut. Der Anbieter weist dem Kunden diese Verpflichtungen auf Anfrage nach.

(3) Zugang zu den im Auftrag verarbeiteten Daten erhalten nur Personen, die ihn zur Erfüllung der vertraglichen Pflichten benötigen. Eine Kenntnisnahme von Einsendungsinhalten erfolgt nur, soweit sie zur Störungsbeseitigung, zur Abwehr von Missbrauch oder zur Ausführung einer Weisung des Kunden erforderlich ist.

(4) Der Anbieter hat keinen Datenschutzbeauftragten bestellt; die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG liegen bei ihm nicht vor. Ansprechpartner für datenschutzrechtliche Fragen aus diesem Vertrag ist der Anbieter selbst unter support@formdall.de.

§ 5 Technische und organisatorische Maßnahmen

TECHNISCHE MASSNAHMEN

(1) Der Anbieter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 28 Abs. 3 lit. c DSGVO). Die bei Inkrafttreten dieser Fassung getroffenen Maßnahmen sind in Anlage 2 beschrieben und werden hiermit vereinbart.

MUSTER

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Anbieter darf sie fortentwickeln, ersetzen oder anpassen, solange das vereinbarte Schutzniveau dabei nicht unterschritten wird. Wesentliche Änderungen dokumentiert der Anbieter durch die Veröffentlichung einer neuen Fassung dieses Vertrags.

(3) Der Kunde hat sich vor Beginn der Verarbeitung von der Angemessenheit der Maßnahmen überzeugt und unterrichtet sich während der Vertragslaufzeit regelmäßig über deren Stand; die dafür vorgesehenen Wege regelt § 10.

(4) Für die Sicherheit in seinem eigenen Verantwortungsbereich hat der Kunde selbst zu sorgen. Das betrifft insbesondere die Wahl sicherer Zugangsdaten, die Aktivierung der angebotenen Zwei-Faktor-Verfahren, die sorgfältige Vergabe von Zugriffsrechten an Mitglieder seines Arbeitsbereichs, die Vertraulichkeit der Signaturschlüssel seiner Webhooks sowie die Absicherung der Systeme, an die er Einsendungen weiterleiten lässt.

§ 6

UNTERAUFTRÄGE

Unterauftragsverarbeiter

(1) Der Kunde erteilt dem Anbieter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen (Art. 28 Abs. 2 Satz 2 DSGVO). Die bei Inkrafttreten dieser Fassung hinzugezogenen Unterauftragsverarbeiter sind in Anlage 1 abschließend aufgeführt; ihrem Einsatz stimmt der Kunde hiermit zu.

MUSTER

(2) Der Anbieter informiert den Kunden über jede beabsichtigte Hinzuziehung eines weiteren oder Ersetzung eines bestehenden Unterauftragsverarbeiters mindestens vier Wochen im Voraus in Textform an die im Konto hinterlegte E-Mail-Adresse. Ist die Frist aus vom Anbieter nicht zu vertretenden Gründen nicht einzuhalten, informiert er unverzüglich.

(3) Der Kunde kann der Änderung innerhalb von vier Wochen ab Zugang der Information aus einem wichtigen, datenschutzrechtlichen Grund widersprechen. Widerspricht der Kunde, so erbringt der Anbieter die Leistung nach Möglichkeit ohne den betreffenden Unterauftragsverarbeiter. Ist ihm das nicht mit zumutbarem Aufwand möglich, können beide Parteien den Nutzungsvertrag nach Maßgabe des § 11 der AGB kündigen; kostenpflichtige Pläne enden dabei zum Ende des laufenden Abrechnungszeitraums. Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Bis zum Wirksamwerden der Kündigung stehen dem Kunden die Exportfunktionen nach § 9 Abs. 3 offen. Widerspricht der Kunde nicht fristgerecht, gilt die Änderung als genehmigt; hierauf weist der Anbieter in der Information nach Absatz 2 hin.

(4) Der Anbieter erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die ihm nach diesem Vertrag obliegen, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO).

MUSTER

Der Anbieter wählt die Unterauftragsverarbeiter sorgfältig aus und überprüft ihre Eignung regelmäßig. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Anbieter dem Kunden gegenüber für dessen Verhalten.

(5) Sämtliche in Anlage 1 genannten Unterauftragsverarbeiter verarbeiten ausschließlich auf Servern in Deutschland. Eine Übermittlung an einen Unterauftragsverarbeiter in einem Drittland findet nicht statt und bedürfte einer Änderung dieses Vertrags.

(6) **Keine Unterauftragsverarbeiter** sind Zieldienste, die der Kunde über einen Connector oder einen Webhook selbst einrichtet, etwa Chat- und Messenger-Dienste oder eigene Endpunkte des Kunden. Die Einrichtung eines solchen Ziels ist eine dokumentierte Weisung nach § 3 Abs. 2, die Übermittlung erfolgt an einen vom Kunden selbst eingesetzten Dienstleister oder an ein eigenes System des Kunden. Für die Rechtsgrundlage der Übermittlung, für ein etwaiges Instrument zur Absicherung einer Drittlandsübermittlung nach Art. 44 ff. DSGVO und für die weitere Verarbeitung im Zieldienst ist allein der Kunde verantwortlich. Dies entspricht § 9 Abs. 2 der AGB.

(7) Ebenfalls keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Nebenleistungen, die nicht die Verarbeitung von Einsendungsdaten betreffen, insbesondere die Zahlungsabwicklung für kostenpflichtige Pläne; Einzelheiten hierzu enthält Anlage 1.

MUSTER

§ 7

BETROFFENENRECHTE

Unterstützung bei Betroffenenrechten

(1) Der Anbieter unterstützt den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte betroffener Personen (Art. 12 bis 23 DSGVO) nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

(2) Die Beantwortung solcher Anträge obliegt dem Kunden als Verantwortlichem. Der Anbieter beantwortet Anträge betroffener Personen nicht eigenständig.

(3) Der Kunde kann Auskunft, Datenübertragbarkeit, Berichtigung und Löschung hinsichtlich der beim Anbieter gespeicherten Einsendungen unmittelbar im Konto ausüben. Der Posteingang erlaubt insbesondere die Suche nach den Einsendungen einer bestimmten Person, deren Anzeige, den Export der gefundenen Einsendungen als CSV-Datei sowie deren endgültige Löschung, einzeln oder für alle Treffer der Suche gemeinsam. Wird die Löschung als Sammellöschung aller Suchtreffer ausgeführt, vermerkt der Anbieter diesen Vorgang im Sicherheitsprotokoll (Zeitpunkt, handelndes Konto, Zahl der gelöschten Einsendungen und ein Hashwert des Suchbegriffs, keine Einsendungsinhalte). Die Löschung einzelner Einsendungen und der CSV-Export werden nicht gesondert protokolliert.

(4) Wendet sich eine betroffene Person unmittelbar an den Anbieter, leitet dieser den Antrag unverzüglich an den Kunden weiter und verweist

MUSTER

die betroffene Person an den Kunden. Der Anbieter erteilt von sich aus keine Auskunft über Einsendungsinhalte und nimmt von sich aus keine Berichtigung oder Löschung vor, es sei denn, der Kunde weist ihn dazu an oder er ist gesetzlich dazu verpflichtet.

(5) Geht die vom Kunden angeforderte Unterstützung über die im Konto verfügbaren Funktionen hinaus und verursacht sie beim Anbieter einen erheblichen Mehraufwand, kann der Anbieter hierfür nach vorheriger Ankündigung eine angemessene Vergütung verlangen. Das gilt nicht, soweit der Mehraufwand auf einem Fehler des Anbieters beruht.

§ 8

MELDEPFLICHTEN

Unterstützung nach Art. 32 bis 36 DSGVO und Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Anbieter unterstützt den Kunden bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen (Art. 28 Abs. 3 lit. f DSGVO).

(2) Der Anbieter meldet dem Kunden jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten, die im Auftrag verarbeitete Daten des Kunden betrifft, unverzüglich nach Kenntniserlangung in Textform an die im Konto hinterlegte E-Mail-Adresse (Art. 33 Abs. 2 DSGVO).

(3) Die Meldung enthält, soweit dem Anbieter bekannt: eine Beschreibung der Art der Verletzung, die betroffenen Kategorien und

MUSTER

die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen der Verletzung sowie die vom Anbieter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und zur Abmilderung möglicher nachteiliger Auswirkungen. Stehen nicht alle Angaben gleichzeitig zur Verfügung, meldet der Anbieter zunächst die verfügbaren Angaben und reicht die übrigen unverzüglich nach.

(4) Die Meldung an die Aufsichtsbehörde nach Art. 33 Abs. 1 DSGVO und die Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO obliegen dem Kunden. Der Anbieter nimmt sie nicht anstelle des Kunden vor, unterstützt ihn dabei aber mit den ihm vorliegenden Informationen.

(5) Der Anbieter ergreift unverzüglich die zur Eindämmung und Behebung erforderlichen Maßnahmen und dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich der ergriffenen Abhilfemaßnahmen.

(6) Auf Anfrage unterstützt der Anbieter den Kunden bei einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und bei einer vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO, indem er die hierfür erforderlichen und ihm vorliegenden Informationen über den Ablauf der Verarbeitung, die eingesetzten Systeme und die getroffenen Maßnahmen bereitstellt.

MUSTER

§ 9

LÖSCHUNG, RÜCKGABE

Löschung und Rückgabe nach Beendigung

(1) Der Anbieter löscht Einsendungen laufend und automatisch nach Ablauf der Aufbewahrungsdauer, die der Kunde für das jeweilige Formular festgelegt hat. Die Löschung erfolgt physisch — die Datensätze werden aus der Datenbank entfernt und nicht lediglich als gelöscht gekennzeichnet — und wird täglich ausgeführt. Die je Plan zulässige Höchstdauer ergibt sich aus der Leistungsbeschreibung; die vom Kunden gewählte Dauer wird auf diese Höchstdauer begrenzt. Diese laufende Löschung ist selbst die Ausführung einer Weisung des Kunden nach § 3 Abs. 2.

(2) Nach Beendigung des Nutzungsvertrags löscht der Anbieter alle im Auftrag verarbeiteten personenbezogenen Daten, oder er gibt sie nach Wahl des Kunden an diesen zurück (Art. 28 Abs. 3 lit. g DSGVO). Trifft der Kunde bis zum Ende des Nutzungsvertrags keine Wahl, werden die Daten gelöscht.

(3) Die Rückgabe erfolgt durch die Bereitstellung der Exportfunktionen im Konto, insbesondere den Export des Posteingangs als CSV-Datei. Der Kunde führt den Export vor Beendigung des Nutzungsvertrags durch; nach Beendigung stehen die Zugänge zum Konto nicht mehr zur Verfügung. Ein darüber hinausgehendes Übergabeformat und eine Übergabe auf einem physischen Datenträger schuldet der Anbieter nicht.

MUSTER

(4) Von der Löschung ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht; ihre Verarbeitung wird für die Dauer der Aufbewahrungspflicht eingeschränkt, und sie werden nach deren Ablauf gelöscht. Einsendungsinhalte unterliegen beim Anbieter keiner gesetzlichen Aufbewahrungspflicht.

(5) Von der laufenden Löschung nach Absatz 1 und von der Löschung nach Absatz 2 nicht erfasst sind Sicherungskopien der Datenbank. Sie werden nach der in Anlage 2 beschriebenen Generationenfolge vorgehalten; eine bereits gelöschte Einsendung kann darin fortbestehen, bis die Kopie, die sie enthält, turnusmäßig ausläuft, längstens 35 Tage. Die Verarbeitung der Sicherungskopien ist auf die Wiederherstellung nach einem Datenverlust beschränkt; sie werden nicht ausgewertet, und einzelne Datensätze werden aus ihnen nicht entnommen. Wird eine Sicherungskopie eingespielt, entfernt der tägliche Löschlauf nach Absatz 1 die darin enthaltenen abgelaufenen Einsendungen automatisch; darüber hinausgehende Löschungen, die der Kunde vor dem Zeitpunkt der Wiederherstellung veranlasst hatte, holt der Anbieter auf dessen Hinweis nach.

(6) Kopien, die auf Weisung des Kunden an von ihm bestimmte Ziele übermittelt wurden — insbesondere an E-Mail-Empfänger, an Webhook-Endpunkte oder an Connector-Zieldienste —, liegen außerhalb des Zugriffs des Anbieters. Ihre Löschung obliegt dem Kunden.

MUSTER

(7) Der Anbieter bestätigt dem Kunden die Löschung nach Absatz 2 auf Anforderung in Textform; die Bestätigung erfolgt unter dem Vorbehalt des Absatzes 5.

§ 10 Nachweise und Überprüfungen

NACHWEISE, PRÜFUNG

(1) Der Anbieter stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind (Art. 28 Abs. 3 lit. h DSGVO). Den Nachweis führt er in erster Linie durch diesen Vertrag einschließlich seiner Anlagen, durch die Datenschutzerklärung sowie durch die öffentlich zugängliche Dokumentation des Dienstes.

(2) Genügen diese Nachweise im Einzelfall nicht, ermöglicht der Anbieter dem Kunden oder einem von diesem beauftragten Prüfer Überprüfungen, einschließlich Inspektionen, und trägt dazu bei. Die Überprüfung erfolgt vorrangig durch Auskünfte in Textform oder durch Fernzugriff und nur, soweit dies nicht ausreicht, vor Ort.

(3) Überprüfungen kündigt der Kunde mit angemessener Frist an, in der Regel vier Wochen. Sie finden während der üblichen Geschäftszeiten statt, dürfen den Betriebsablauf nicht unangemessen stören und erfolgen höchstens einmal je Kalenderjahr. Bei einem besonderen Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten oder auf Verlangen einer Aufsichtsbehörde, sind Überprüfungen auch kurzfristiger und häufiger zulässig.

MUSTER

(4) Die Kosten seiner Überprüfung trägt der Kunde. Für den Aufwand einer Überprüfung vor Ort kann der Anbieter eine angemessene Vergütung verlangen; das gilt nicht, wenn die Überprüfung einen Verstoß des Anbieters gegen diesen Vertrag aufdeckt.

(5) Ein beauftragter Prüfer darf kein Wettbewerber des Anbieters sein und ist vor der Überprüfung zur Verschwiegenheit zu verpflichten. Der Anbieter kann Auskünfte insoweit verweigern, als sie Geschäftsgeheimnisse offenlegen oder personenbezogene Daten anderer Kunden preisgeben würden; eine Überprüfung darf nicht dazu führen, dass der Kunde Zugang zu Daten anderer Kunden erhält.

(6) Der Anbieter unterrichtet den Kunden unverzüglich über Kontrollen und Maßnahmen einer Aufsichtsbehörde, soweit sie die Verarbeitung im Auftrag des Kunden betreffen.

§ 11

HAFTUNG, SCHLUSS

Haftung, Schlussbestimmungen und Sprachenvorrang

(1) Für die Haftung der Parteien untereinander gelten die Regelungen des Nutzungsvertrags, insbesondere § 12 der AGB. Art. 82 DSGVO und die Haftung gegenüber betroffenen Personen bleiben davon unberührt.

(2) Dieser Vertrag wird mit der Annahme der AGB als Bestandteil des Nutzungsvertrags wirksam; ein gesonderter Abschluss ist nach § 9 Abs. 1 der AGB nicht erforderlich. Er gilt vom Beginn des Nutzungsvertrags an für dessen gesamte Dauer.

MUSTER

(3) Der Vertrag wird in elektronischer Form geschlossen und bereitgestellt. Art. 28 Abs. 9 DSGVO lässt die elektronische Form ausdrücklich zu; eine eigenhändige Unterschrift ist zur Wirksamkeit nicht erforderlich, und das Dokument trägt deshalb keine Unterschriften. Der Kunde kann den vollständigen Vertragstext jederzeit in seinem Konto einsehen und als PDF herunterladen.

(4) Bei Widersprüchen zwischen diesem Vertrag und den AGB gehen in allen Fragen der Verarbeitung personenbezogener Daten im Auftrag die Regelungen dieses Vertrags vor. Im Übrigen bleiben die AGB unberührt. Allgemeine Geschäftsbedingungen des Kunden werden nicht Bestandteil dieses Vertrags.

(5) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform; das gilt auch für die Änderung dieser Klausel. Änderungen erfolgen durch die Veröffentlichung einer neuen, datierten Fassung. Eine veröffentlichte Fassung wird nicht rückwirkend geändert. Welche Fassung für den Kunden gilt, weist sein Konto aus; frühere Fassungen bleiben dort abrufbar.

(6) Sollte eine Bestimmung dieses Vertrags unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung. Entsprechendes gilt für Regelungslücken.

MUSTER

(7) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Zwingende Verbraucherschutzvorschriften des Staates, in dem ein Kunde als Verbraucher seinen gewöhnlichen Aufenthalt hat, bleiben unberührt.

(8) Maßgeblich ist die deutsche Fassung dieses Vertrags. Eine englische Übersetzung dient allein dem Verständnis; bei Abweichungen zwischen den Sprachfassungen geht die deutsche Fassung vor.

Anlage 1

UNTERAUFTRÄGE

Unterauftragsverarbeiter

Der Anbieter setzt für die Verarbeitung im Auftrag des Kunden die folgenden Unterauftragsverarbeiter ein. Die Liste ist mit der Subunternehmerliste in der Datenschutzerklärung des Anbieters deckungsgleich und bei Inkrafttreten dieser Fassung abschließend.

MUSTER

Unternehmen	Anschrift	Leistung	Standort
netcup GmbH	Daimlerstraße 25, 90441 Nürnberg, Deutschland	Hosting der Website formdall.de. Über diese Website werden keine Einsendungsdaten verarbeitet.	Deutschland
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting des Dienstes (app.formdall.de, api.formdall.de) einschließlich Anwendungsservern und Datenbank. Hier werden die Einsendungen gespeichert.	Deutschland

Unternehmen	Anschrift	Leistung	Standort
Contabo GmbH	Aschauer Straße 32a, 81549 München, Deutschland	Betrieb des Mailservers für Benachrichtigungen, automatische Antworten und System-E-Mails.	Deutschland

Sämtliche Unterauftragsverarbeiter verarbeiten ausschließlich auf Servern in Deutschland. Eine Übermittlung in ein Drittland findet nicht statt. Weitere Unterauftragsverarbeiter für die Verarbeitung von Einsendungen setzt der Anbieter nicht ein.

Zahlungsabwicklung: Creem – kein Unterauftragsverarbeiter

Zahlungen für kostenpflichtige Pläne werden über Creem abgewickelt. Creem tritt als Merchant of Record auf, wird also gegenüber dem Kunden selbst Vertragspartner des Kaufvorgangs und ist für die Verarbeitung der Zahlungs-, Rechnungs- und Steuerdaten eigener Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Creem ist deshalb kein Unterauftragsverarbeiter des Anbieters und steht bewusst nicht in der vorstehenden Tabelle.

Einsendungen und deren Inhalte werden zu keinem Zeitpunkt an Creem übermittelt. Die Zahlungsabwicklung berührt die Verarbeitung im Auftrag nach diesem Vertrag nicht. Für die Verarbeitung durch Creem gelten dessen eigene Datenschutzhinweise; sie betrifft Daten des Kunden, nicht Daten der Einsender.

MUSTER

Vom Kunden eingerichtete Zieldienste – keine Unterauftragsverarbeiter

Richtet der Kunde für ein Formular einen Connector oder einen Webhook ein, werden die von ihm ausgewählten Felder der Einsendung an das von ihm bestimmte Ziel übermittelt, etwa an einen Chat-Dienst wie Slack oder Discord oder an einen eigenen Endpunkt des Kunden. Diese Zieldienste sind keine Unterauftragsverarbeiter des Anbieters, sondern vom Kunden selbst eingesetzte Dienstleister oder Systeme des Kunden; zwischen dem Anbieter und dem Betreiber des Zieldienstes besteht insoweit kein Vertragsverhältnis. Die Einrichtung ist eine dokumentierte Weisung nach § 3 Abs. 2. Ohne Einrichtung durch den Kunden findet keine Weiterleitung statt.

Offengelegte Übermittlungen bei der Spam- und Missbrauchsabwehr

Zur Abwehr von Spam gleicht der Anbieter die IP-Adresse des Einsenders zunächst gegen eine bei ihm lokal vorgehaltene Sperrliste ab; bei diesem Abgleich werden keine Daten nach außen übermittelt. Nur wenn der lokale Abgleich keinen Treffer ergibt, fragt der Anbieter zusätzlich eine DNS-basierte Blockliste ab. Bei dieser Abfrage wird die IP-Adresse des Einsenders technisch bedingt an den eingesetzten DNS-Resolver und an den Betreiber der Blockliste übermittelt. Weitere Daten der Einsendung, insbesondere Feldinhalte, werden dabei nicht übertragen.

MUSTER

Der Anbieter legt diese Übermittlung hiermit offen. Sie begründet nach Auffassung der Parteien kein Auftragsverhältnis, weil der Betreiber der Blockliste die Abfrage zu eigenen Zwecken beantwortet und nicht auf Weisung des Anbieters tätig wird. Die Abfrage ist Bestandteil der Spam-Abwehr des Dienstes und lässt sich nicht je Formular abschalten.

Aktiviert der Kunde für ein Formular die Prüfung auf zustellbare E-Mail-Adressen, so löst der Anbieter zusätzlich den Domain-Teil der vom Einsender angegebenen E-Mail-Adresse im Domain Name System auf (MX-Eintrag, ersatzweise A-Eintrag). Dabei wird dieser Domain-Teil, also ein Bestandteil eines Formularfelds, an den eingesetzten DNS-Resolver übermittelt. Der Teil der E-Mail-Adresse vor dem Trennzeichen und alle übrigen Feldinhalte werden dabei nicht übertragen. Ohne diese Einstellung findet die Abfrage nicht statt; die Einrichtung der Einstellung ist eine dokumentierte Weisung nach § 3 Abs. 2.

Wählt der Kunde für sein Formular ein Captcha-Verfahren eines Drittanbieters, so übermittelt der Anbieter zu dessen serverseitiger Prüfung ausschließlich das im Browser des Einsenders erzeugte Lösungs-Token sowie die vom Kunden hinterlegten Schlüssel an diesen Drittanbieter; Feldinhalte und die IP-Adresse des Einsenders übermittelt der Anbieter dabei nicht. Wählt der Kunde kein Captcha oder das vom Anbieter selbst betriebene Proof-of-Work-Verfahren, findet keine Übermittlung an Dritte statt. Welche Daten der Browser des Einsenders unmittelbar an den Drittanbieter sendet, richtet sich nach dessen

MUSTER

Einbindung durch den Kunden und liegt außerhalb des Einflussbereichs des Anbieters.

Der Abgleich gegen Wegwerf-E-Mail-Domains erfolgt ausschließlich gegen eine beim Anbieter lokal vorgehaltene Liste; dabei werden keine Daten übermittelt. Einsendungsdaten verlassen die Infrastruktur des Anbieters ausschließlich in den in diesem Abschnitt genannten Fällen sowie auf dem Weg an die vom Kunden bestimmten Ziele — insbesondere an die von ihm hinterlegten E-Mail-Empfänger, an den Einsender selbst bei einer von ihm eingerichteten automatischen Antwort, an Webhook-Endpunkte und an Connector-Zieldienste. Darüber hinaus findet keine Übermittlung statt.

Anlage 2

TECHNISCHE MASSNAHMEN

Technische und organisatorische Maßnahmen

Die folgenden Maßnahmen sind zum Zeitpunkt des Inkrafttretens dieser Fassung umgesetzt. Aufgenommen sind nur Maßnahmen, die im Dienst tatsächlich implementiert sind; Absichtserklärungen enthält diese Anlage bewusst nicht.

MUSTER

Maßnahme	Umsetzung
Vertraulichkeit der Einsendungsinhalte	Die Inhalte einer Einsendung werden ausschließlich verschlüsselt in der Datenbank abgelegt (AES-256 mit dem anwendungseigenen Schlüssel). Ein Zugriff auf die Datenbank allein gibt die Feldinhalte nicht preis.

Maßnahme	Umsetzung
Pseudonymisierung der IP-Adressen von Einsendern	Zur Einsendung wird die IP-Adresse des Einsenders nicht im Klartext gespeichert, sondern nur gehasht (HMAC-SHA-256 mit einem täglich wechselnden Zufallswert). Auch die Zwischenspeicherung bei der Spam-Abwehr erfolgt ausschließlich über einen Schlüssel, der die IP-Adresse gehasht enthält.
Keine Dateianhänge	Der Dienst nimmt keine Datei-Uploads entgegen und speichert keine Dateien von Einsendern. Es existiert kein Verarbeitungspfad für hochgeladene Dateien.
Speicherbegrenzung durch Aufbewahrungsfristen	Jede Einsendung erhält beim Eingang einen Verfallszeitpunkt aus der vom Kunden je Formular gewählten Aufbewahrungsdauer. Diese wird auf die planabhängige Höchstdauer begrenzt: 14 Tage im Free-Plan, 90 Tage im Hobby-Plan und 365 Tage in den übrigen kostenpflichtigen Plänen. Der Kunde kann die Speicherung je Formular auch vollständig abschalten.
Tägliche physische Löschung	Ein täglich ausgeführter Auftrag entfernt abgelaufene Einsendungen und die zugehörigen Zustellprotokolle endgültig aus der Datenbank; es findet keine bloße Markierung als gelöscht statt. Die Löschung wirkt sofort im Produktivsystem; in den Sicherungen nach der Zeile „Verfügbarkeit und Wiederherstellbarkeit“ endet sie mit dem Auslaufen der betroffenen Kopie (§ 9 Abs. 5).
Löschung fehlgeschlagener Hintergrundaufträge	Fehlgeschlagene Hintergrundaufträge können in ihrem gespeicherten Auftragsinhalt personenbezogene Daten enthalten; sie werden täglich gelöscht, sobald sie älter als 72 Stunden sind.

MUSTER

Maßnahme	Umsetzung
Zugangskontrolle zum Konto	Passwörter werden ausschließlich als kryptographischer Hash gespeichert. Zusätzlich stehen eine Zwei-Faktor-Authentisierung per TOTP mit Wiederherstellungscodes sowie Passkeys nach dem WebAuthn-Standard zur Verfügung. Anmeldung, Zwei-Faktor-Bestätigung und Passkey-Anmeldung sind gegen wiederholte Versuche ratenbegrenzt. E-Mail-Adressen werden vor der Nutzung verifiziert.
Zugriffskontrolle und Mandantentrennung	Jedes Formular und jede Einsendung gehört zu genau einem Arbeitsbereich. Jeder Zugriff wird über die Mitgliedschaft im Arbeitsbereich und ein abgestuftes Rollen- und Rechtekonzept geprüft (Inhaber, Administrator, Mitglied; je Formular zusätzlich Verwalter, Bearbeiter oder nur Lesezugriff). Das Lesen von Einsendungsinhalten ist von der Formularverwaltung getrennt berechtigt. Ein Zugriff über Arbeitsbereichsgrenzen hinweg ist damit ausgeschlossen.
Transportverschlüsselung und Sicherheitskopfzeilen	Der Dienst wird über HTTPS bereitgestellt; die Verbindungen zu app.formdall.de und api.formdall.de sind TLS-verschlüsselt. Die Weboberfläche (das Kundenkonto unter app.formdall.de) wird zusätzlich durch Sicherheitskopfzeilen abgesichert, die insbesondere das Erraten von Inhaltstypen, die Einbettung in fremde Seiten und die Weitergabe von Aufrufinformationen an fremde Ziele unterbinden; außerhalb der lokalen Entwicklungsumgebung liefert sie darüber hinaus eine Content-Security-Policy aus, die fremde Einbettung, fremde Formularziele und fremde Skriptquellen unterbindet. Die Einsendungsschnittstelle unter api.formdall.de ist dafür bestimmt, aus fremden Websites heraus aufgerufen zu werden, und stellt keine im Browser dargestellte Oberfläche bereit; diese Kopfzeilen werden dort deshalb nicht gesetzt. Ihr Schutz beruht auf der Transportverschlüsselung und auf der in dieser Anlage beschriebenen Eingabe- und Missbrauchskontrolle.

MUSTER

Maßnahme	Umsetzung
Geschützte Ablage von Zugangsdaten und Schlüsseln	Zugangs-Token für Connectoren und die Signaturschlüssel für Webhooks werden verschlüsselt und getrennt von den Einsendungsinhalten gespeichert. Webhook-Auslieferungen werden mit einer HMAC-SHA-256-Signatur versehen, damit der Empfänger ihre Echtheit prüfen kann.
Eingabe- und Missbrauchskontrolle	Die Annahme einer Einsendung durchläuft eine feste Prüfkette: Prüfung des zulässigen Ursprungs, Begrenzung von Nachrichtengröße, Feldzahl und Feldlänge, Erkennung doppelter Einsendungen, Honeypot, Captcha, Abgleich der IP-Reputation, Prüfung gegen ein vom Kunden festgelegtes Feldschema, Erkennung von Wegwerf-E-Mail-Adressen und Kontingentprüfung. Die Einsendungsschnittstelle ist zusätzlich ratenbegrenzt.
Protokollierung sicherheitsrelevanter Vorgänge	Protokolliert werden mit Zeitpunkt, Ereignisart, handelndem Konto und gehashter IP-Adresse: erfolgreiche Anmeldungen; Änderungen an Passwort, Zwei-Faktor-Authentisierung und Passkeys; Profiländerungen; die Löschung des Kontos; der Widerruf erteilter Anwendungszugriffe; Einladung, Widerruf einer Einladung, Beitritt, Rollenwechsel und Entfernen von Mitgliedern sowie die Übertragung der Inhaberschaft; die Vergabe und der Entzug formularbezogener Zugriffsrechte; die Änderung der in diesem Vertrag genannten Angaben zum Verantwortlichen; die Sammellöschung von Einsendungen im Rahmen eines Betroffenenantrags; sowie abrechnungs- und administrationsbezogene Vorgänge. Nicht protokolliert werden inhaltliche Änderungen an Formularen, Exporte und die Löschung einzelner Einsendungen. Das Protokoll enthält keine Passwörter, keine Zugangsdaten und keine Einsendungsinhalte.

MUSTER

Maßnahme	Umsetzung
Unterstützung der Betroffenenrechte	Im Konto stehen Suche, Anzeige, CSV-Export und endgültige Löschung der Einsendungen einer bestimmten Person bereit, einzeln oder für alle Treffer der Suche gemeinsam. Die Sammellöschung aller Suchtreffer wird im Sicherheitsprotokoll vermerkt; die Löschung einzelner Einsendungen und der Export werden nicht gesondert protokolliert.
Verfügbarkeit und Wiederherstellbarkeit	Von der Datenbank wird jede Nacht eine vollständige Sicherung erstellt. Sie wird bereits auf dem Server verschlüsselt, bevor sie ihn verlässt, und zwar mit einem öffentlichen Schlüssel: auf dem Server liegt damit kein Schlüssel, mit dem sich eine Sicherung lesen ließe. Eine unverschlüsselte Kopie wird zu keinem Zeitpunkt auf dem Server abgelegt. Die privaten Schlüssel, die eine Sicherung öffnen können, werden getrennt vom Server und getrennt von den Sicherungen verwahrt. Die Sicherung wird nicht vom Server versendet, sondern vom Sicherungsgerät abgeholt; der Server kennt dieses Gerät nicht und kann von sich aus keine Verbindung zu ihm aufbauen. Wer die Kontrolle über den Server erlangt, kann bereits erstellte Sicherungen deshalb weder lesen noch verändern oder löschen. Der für die Abholung verwendete Zugang ist technisch auf den einen Vorgang „Sicherung einer Datenbank erstellen“ beschränkt. Vorgehalten werden sieben tägliche und vier wöchentliche Sicherungen; zusätzlich besteht eine Zweitkopie auf einem getrennten Datenträger. Der nächtliche Lauf wird durch einen von der Sicherung unabhängigen Dienst überwacht, der auch das Ausbleiben einer Sicherung meldet; an ihn werden keine Einsendungsdaten übermittelt. Die Wiederherstellbarkeit ist durch eine vollständige Probewiederherstellung geprüft.

MUSTER

Maßnahme	Umsetzung
Verarbeitung ausschließlich in Deutschland	Anwendung, Datenbank und Mailserver werden ausschließlich auf Servern in Deutschland betrieben. Die Sicherungen der Datenbank und die Zweitkopie werden auf Geräten des Anbieters an dessen im Rubrum genannter Anschrift in Deutschland verwahrt; ein Dritter ist damit nicht befasst. Die eingesetzten Unterauftragsverarbeiter sind in Anlage 1 benannt.
Trennung nach Zweck	Daten des Kundenkontos, Einsendungsdaten, Zustellprotokolle und das Sicherheitsprotokoll werden getrennt geführt. Zahlungsdaten verarbeitet der Anbieter nicht selbst; sie liegen beim Zahlungsdienstleister als eigenem Verantwortlichen.

Ende des Vertrags. Fassung 2026-08-21.

MUSTER