

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO – Feedcube

Fassung 1.1 · Stand 11.10.2026

zwischen

dem Kunden, der mit dem Auftragnehmer einen Vertrag über die Nutzung von Feedcube geschlossen hat,
Name bzw. Firma und Anschrift:

– nachfolgend „Auftraggeber“ (Verantwortlicher) –

und

Dominic Koch, Einzelunternehmer, Kochsoftware

Schönreitherstraße 31a, 4224 Wartberg ob der Aist, Österreich

GISA-Zahl 37215897, E-Mail office@feedcube.net

– nachfolgend „Auftragnehmer“ (Auftragsverarbeiter) –

– gemeinsam „Parteien“ –

Präambel

Der Auftraggeber nutzt die Feedback- und Umfrageplattform Feedcube, die der Auftragnehmer als Software-as-a-Service bereitstellt. Grundlage ist der Vertrag über die Nutzung von Feedcube, für den die Allgemeinen Geschäftsbedingungen des Auftragnehmers (AGB) gelten (nachfolgend „Hauptvertrag“), gleich ob die Nutzung entgeltlich oder unentgeltlich erfolgt.

Diese Vereinbarung regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien nach Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO) und dem österreichischen Datenschutzgesetz (DSG). Sie gilt unabhängig davon, wofür der Auftraggeber Feedcube einsetzt, etwa für Kunden-, Kurs- und Seminar- oder Mitarbeitendenfeedback.

§ 1 Gegenstand, Geltungsbereich, Dauer und Ort der Verarbeitung

- (1) Der Auftragnehmer stellt Feedcube für den Auftraggeber bereit und übernimmt Betrieb, Hosting, Wartung und Support. Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen beschreibt Anlage 1.
- (2) Diese Vereinbarung gilt für Feedcube. Der Auftragnehmer betreibt Feedcube auf einer gemeinsamen Plattform mit seinen weiteren Produkten CourseMate, Quipla und Mindsketch. Für den Auftraggeber richtet er einen eigenen Mandanten mit eigener Datenbank ein; innerhalb dieses Mandanten nutzen die Produkte dieselbe Datenbank, dieselben Benutzerkonten und dieselbe Anmeldung. Gemeinsam genutzte Daten wie die Benutzerkonten fallen unter diese Vereinbarung, soweit sie für Feedcube verarbeitet werden. Verarbeitungen in den weiteren Produkten sind nicht Gegenstand dieser Vereinbarung. Bucht der Auftraggeber eines dieser Produkte, vereinbaren die Parteien dafür eine gesonderte Ergänzung, die die zusätzlichen Verarbeitungen, Unterauftragsverarbeiter und Fristen festlegt. Die weiteren Produkte sind im Mandanten technisch erreichbar, auch wenn der Auftraggeber sie nicht gebucht hat, und Rollen, insbesondere vorgegebene Standardrollen, können Berechtigungen für sie enthalten. Der Auftraggeber kann nicht gebuchte Produkte in den Einstellungen deaktivieren; sie werden dann nicht mehr zur Auswahl angeboten. Er weist seine Benutzer an, nicht gebuchte Produkte

nicht zu nutzen. Werden dort dennoch personenbezogene Daten des Auftraggebers verarbeitet, verarbeitet der Auftragnehmer sie nur im Auftrag und nach Weisung des Auftraggebers; die §§ 2, 4, 5 und 7 bis 11 gelten entsprechend.

- (3) Nicht Gegenstand dieser Vereinbarung sind Daten, die der Auftragnehmer als Verantwortlicher verarbeitet, insbesondere Vertrags-, Abrechnungs- und Kontaktdaten des Auftraggebers und seiner Ansprechpersonen sowie die Kommunikation mit ihnen, auch zu Supportanfragen. Daten aus Feedcube, die der Auftragnehmer bei der Bearbeitung von Supportanfragen einsieht oder die ihm dabei übermittelt werden, verarbeitet er dagegen ausschließlich im Auftrag und nach dieser Vereinbarung.
- (4) Diese Vereinbarung ist Bestandteil des Hauptvertrags. Sie wird wirksam, wenn der Auftraggeber den Hauptvertrag unter Einbeziehung der AGB abschließt, die auf diese Vereinbarung verweisen; der Abschluss in elektronischer Form genügt (Art. 28 Abs. 9 DSGVO). Auf Wunsch unterzeichnen die Parteien sie zusätzlich, auch elektronisch. Wird sie erst während der Laufzeit des Hauptvertrags abgeschlossen, wird sie mit ihrer Annahme oder Unterzeichnung wirksam und gilt auch für die Daten, die der Auftragnehmer zuvor im Rahmen des Hauptvertrags verarbeitet hat. Sie gilt für die Dauer des Hauptvertrags und darüber hinaus, solange der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet oder in seinem Besitz hat.
- (5) Die Daten des Auftraggebers werden in Rechenzentren in der Europäischen Union gespeichert und verarbeitet; Ausnahmen sind in Anlage 3 ausgewiesen. Ist bei einem Unterauftragsverarbeiter eine Verarbeitung in einem Drittland oder ein Zugriff von dort nicht ausgeschlossen, nennt Anlage 3 die Grundlage nach Kapitel V DSGVO, also einen Angemessenheitsbeschluss (Art. 45 DSGVO) oder geeignete Garantien wie Standardvertragsklauseln (Art. 46 DSGVO).
- (6) Für neue Unterauftragsverarbeiter mit Drittlandbezug gilt das Verfahren nach § 6; die Information nennt die Grundlage nach Kapitel V DSGVO. Eine Verlagerung der Datenbank des Auftraggebers in ein Drittland bedarf seiner vorherigen Zustimmung in schriftlicher oder elektronischer Form (z. B. E-Mail).
- (7) Entfällt eine in Anlage 3 genannte Grundlage, etwa weil ein Angemessenheitsbeschluss aufgehoben wird oder ausläuft, informiert der Auftragnehmer den Auftraggeber unverzüglich und stützt die Übermittlung auf eine andere Grundlage nach Kapitel V DSGVO; ist das nicht möglich, stellt er die betroffene Übermittlung ein. Verlangt eine Behörde oder ein Gericht eines Drittlands die Herausgabe von Daten des Auftraggebers, unterrichtet er den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist, und gibt Daten nur nach Maßgabe von Art. 48 DSGVO heraus.

§ 2 Weisungen des Auftraggebers

- (1) Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers; das gilt auch für Übermittlungen in ein Drittland oder an eine internationale Organisation (Art. 28 Abs. 3 lit. a DSGVO). Verpflichtet ihn das Recht der Union oder eines Mitgliedstaats zu einer anderen Verarbeitung, teilt er dem Auftraggeber diese Verpflichtung vorher mit, es sei denn, das betreffende Recht untersagt die Mitteilung aus wichtigen Gründen des öffentlichen Interesses.
- (2) Die Weisungen ergeben sich aus dem Hauptvertrag, dieser Vereinbarung samt Anlagen sowie aus den Einstellungen und Aktionen, die der Auftraggeber und die von ihm berechtigten Personen in Feedcube vornehmen, etwa dem Anlegen und Versenden von Umfragen, der Auswahl der Eingeladenen, der Vergabe von Rollen und Berechtigungen, dem Einstellen der Schwellen und der Nutzung optionaler Funktionen. Ob und wofür seine Benutzer die optionalen KI-Funktionen verwenden, entscheidet der Auftraggeber; er kann sie für seinen Mandanten in den Einstellungen insgesamt abschalten. Welche Berechtigungen die einzelnen KI-Funktionen voraussetzen, beschreibt Anlage 1

Abschnitt 6 e; eine eigene Berechtigung, mit der sich die KI-Funktionen auf einzelne Rollen oder Personen beschränken lassen, bietet Feedcube nicht.

- (3) Einzelweisungen erteilt der Auftraggeber schriftlich oder in elektronischer Form (z. B. E-Mail) an die Adresse nach § 13. In dringenden Fällen kann er sie mündlich erteilen und bestätigt sie dann unverzüglich in dieser Form. Der Auftragnehmer dokumentiert Einzelweisungen und ihre Umsetzung. Weisungen, die über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen, behandeln die Parteien als Wunsch nach einer Leistungsänderung; Weisungen nach § 7, § 9 und § 11 bleiben davon unberührt.
- (4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen Datenschutzrecht der Union oder eines Mitgliedstaats verstößt, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert. Eine offensichtlich rechtswidrige Weisung muss er auch nach Bestätigung nicht ausführen.
- (5) Der Auftragnehmer verwendet die Daten nur, um die vereinbarten Leistungen zu erbringen, und nicht für eigene Zwecke. Er nutzt sie insbesondere nicht für Werbung, zur Profilbildung, zum Training von KI-Modellen oder für Auswertungen über mehrere Kunden hinweg; ausgenommen ist die Auswertung technischer Daten, soweit sie für Betrieb und Sicherheit von Feedcube erforderlich ist.

§ 3 Pflichten des Auftraggebers

- (1) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für das Vorliegen einer Rechtsgrundlage, für die Information der betroffenen Personen nach Art. 13 und 14 DSGVO und für die Wahrung ihrer Rechte.
- (2) Der Auftraggeber stellt insbesondere sicher, dass
 - a) für die Befragungen eine Rechtsgrundlage besteht und Beteiligungs- oder Zustimmungsrechte gewahrt sind, etwa die einer Arbeitnehmervertretung, wenn Beschäftigte befragt oder bewertet werden,
 - b) die Teilnehmenden vor der Teilnahme über Zweck, Freiwilligkeit, Anonymität oder Personenbezug und die Art der Auswertung informiert werden, einschließlich eines etwaigen Einsatzes von KI-Funktionen,
 - c) Fragen, Auswertungseinheiten, Schuttschwellen und Berechtigungen so gewählt werden, dass die in Anlage 1 Abschnitt 6 beschriebenen Schutzvorkehrungen wirksam bleiben und Zusagen an die Teilnehmenden, insbesondere zur Anonymität, eingehalten werden,
 - d) Zugänge und Berechtigungen nur Personen erhalten, die sie für ihre Aufgaben benötigen, und Konten ausgeschiedener Personen zeitnah deaktiviert oder gelöscht werden,
 - e) Ergebnisse der KI-Funktionen vor ihrer Verwendung geprüft und weder zur Beurteilung von Leistung oder Verhalten einzelner Personen noch als Grundlage für Entscheidungen über einzelne Personen herangezogen werden,
 - f) KI-Funktionen nicht auf Auswahlen angewendet werden, die Antworten aus Befragungen enthalten, an denen Minderjährige teilnehmen, die auf Angaben über Minderjährige abzielen oder in denen staatliche Identifikationsnummern oder Zahlungskartendaten abgefragt werden; bei Befragungen mit besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) nur nach vorheriger Abstimmung mit dem Auftragnehmer (Anlage 1 Abschnitt 5; Anlage 3 Abschnitt 1 Abs. 5).

- (3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er bei der Verarbeitung Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen feststellt.

§ 4 Vertraulichkeit

- (1) Der Auftragnehmer setzt für die Verarbeitung nur Personen ein, die seinen Weisungen unterstehen (Art. 29 DSGVO) und vertraglich oder kraft Gesetzes zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b DSGVO). Seine Mitarbeiterinnen und Mitarbeiter verpflichtet er vor Aufnahme ihrer Tätigkeit vertraglich auf das Datengeheimnis nach § 6 DSG, auch für die Zeit nach dem Ende ihres Dienst- oder Auftragsverhältnisses, und belehrt sie über die für sie geltenden Weisungen und die Folgen von Verstößen. Er selbst wahrt das Datengeheimnis ebenso.
- (2) Zugriff auf Daten des Auftraggebers erhalten nur Personen, die ihn für Betrieb, Wartung, Sicherheit oder Support von Feedcube benötigen, und nur im erforderlichen Umfang. Die Pflicht zur Vertraulichkeit gilt nach Ende dieser Vereinbarung fort.

§ 5 Sicherheit der Verarbeitung

- (1) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen, die Art. 32 DSGVO verlangt, und richtet sie am Risiko der Verarbeitung aus. Den bei Abschluss dieser Vereinbarung geltenden Stand beschreibt Anlage 2.
- (2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer überprüft sie regelmäßig und darf sie durch gleichwertige oder wirksamere Maßnahmen ersetzen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber auf Anfrage mit.

§ 6 Unterauftragsverarbeiter

- (1) Der Auftraggeber genehmigt allgemein, dass der Auftragnehmer die in Anlage 3 genannten Unterauftragsverarbeiter einsetzt (Art. 28 Abs. 2 DSGVO). Die Genehmigung umfasst die weiteren Unterauftragsverarbeiter, die diese Anbieter ihrerseits einsetzen und in eigenen Listen führen. Die aktuelle Fassung der Anlage 3 und diese Listen stellt der Auftragnehmer auf Anfrage zur Verfügung.
- (2) Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage im Voraus schriftlich oder in elektronischer Form, bevor er einen weiteren Unterauftragsverarbeiter hinzuzieht, einen bestehenden ersetzt oder bei einem bestehenden den Ort der Verarbeitung oder die übermittelten Datenkategorien wesentlich ändert. Die Information nennt Name und Anschrift, Leistung, betroffene Daten, Ort der Verarbeitung und gegebenenfalls die Grundlage für die Übermittlung in ein Drittland. Muss ein Unterauftragsverarbeiter kurzfristig ersetzt werden, etwa weil er seine Leistung einstellt oder seine Datenschutzpflichten verletzt, kann die Frist angemessen kürzer sein. Über Änderungen bei den weiteren Unterauftragsverarbeitern nach Absatz 1 Satz 2 informiert der Auftragnehmer unverzüglich, nachdem er davon Kenntnis erlangt hat.
- (3) Der Auftraggeber kann einer Änderung innerhalb von 14 Tagen nach Zugang der Information schriftlich oder in elektronischer Form unter Angabe von Gründen widersprechen. Die Parteien suchen dann eine einvernehmliche Lösung. Gelingt das nicht, kann der Auftraggeber den Hauptvertrag und diese Vereinbarung mit Wirkung zum Zeitpunkt der Änderung außerordentlich kündigen; im Voraus bezahlte Entgelte für die Zeit danach erstattet der Auftragnehmer anteilig. Widerspricht der Auftraggeber nicht fristgerecht, gilt die Änderung als genehmigt.

- (4) Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig aus und erlegt ihnen vertraglich im Wesentlichen dieselben Datenschutzpflichten auf, die diese Vereinbarung vorsieht, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Auf Verlangen stellt er dem Auftraggeber eine Kopie der datenschutzrelevanten Vertragsbestimmungen zur Verfügung; Geschäftsgeheimnisse darf er schwärzen, und bei öffentlich abrufbaren Standardbedingungen genügt der Hinweis auf die Fundstelle. Erfährt er, dass ein Unterauftragsverarbeiter seine Datenschutzpflichten in Bezug auf Daten des Auftraggebers verletzt, unterrichtet er den Auftraggeber; § 9 bleibt unberührt. Für die Erfüllung der Pflichten seiner Unterauftragsverarbeiter haftet der Auftragnehmer dem Auftraggeber wie für eigenes Verhalten.
- (5) Keine Unterauftragsverarbeitung sind Leistungen, bei denen der Dienstleister keinen Zugriff auf personenbezogene Daten des Auftraggebers erhält, etwa die Übertragung verschlüsselter Daten durch Telekommunikationsanbieter. Der Auftragnehmer trifft auch dort angemessene Vorkehrungen zum Schutz der Daten.

§ 7 Unterstützung bei Betroffenenrechten

- (1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten, insbesondere auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Soweit Feedcube dafür Funktionen bietet, etwa zum Auffinden, Exportieren und Löschen von Daten, nutzt der Auftraggeber zunächst diese.
- (2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser ihren Antrag innerhalb von drei Arbeitstagen (Montag bis Freitag, ausgenommen gesetzliche Feiertage in Österreich) an den Auftraggeber weiter, sofern er den Antrag dem Auftraggeber zuordnen kann. Er beantwortet den Antrag nicht selbst, es sei denn, der Auftraggeber weist ihn dazu an.
- (3) Feedcube speichert Antworten ohne Benutzerkennung, E-Mail-Adresse und IP-Adresse der antwortenden Person. Ob sich eine Antwort einer Person zuordnen lässt, hängt vom Einzelfall ab, insbesondere von Organisationsmerkmalen, Freitexten und der Größe der befragten Gruppe (Anlage 1 Abschnitt 6 a). Kann der Auftraggeber die antwortende Person nicht identifizieren, gilt Art. 11 DSGVO; macht die Person zusätzliche Angaben, die eine Zuordnung ermöglichen, etwa zu Wortlaut oder Zeitpunkt ihrer Antwort, sind ihre Rechte nach Art. 15 bis 20 DSGVO zu erfüllen (Art. 11 Abs. 2 DSGVO). Zusätzliche Informationen, um antwortende Personen zu identifizieren, werden allein zu diesem Zweck weder erhoben noch aufbewahrt (Art. 11 Abs. 1 DSGVO).
- (4) Antworten, in denen eine Person bewertet oder genannt wird, sind auch deren personenbezogene Daten; ihre Rechte bleiben unberührt. Beantragt eine solche Person Auskunft, legt der Auftraggeber fest, wie die Rechte und Freiheiten der antwortenden Personen gewahrt werden (Art. 15 Abs. 4 DSGVO), etwa indem Zeitpunkte und andere Merkmale weggelassen werden, die auf die antwortende Person schließen lassen, und indem Freitexte vor der Herausgabe geprüft werden. Der Auftragnehmer stellt die Daten auf Weisung in dieser Form bereit.

§ 8 Weitere Unterstützungspflichten

- (1) Soweit es die Art der Verarbeitung und die ihm vorliegenden Informationen zulassen, unterstützt der Auftragnehmer den Auftraggeber bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen und einer etwaigen vorherigen Konsultation der

Aufsichtsbehörde. Er stellt dafür die erforderlichen Angaben zu den Verarbeitungsvorgängen, den technischen und organisatorischen Maßnahmen und den Unterauftragsverarbeitern bereit.

- (2) Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt dem Auftraggeber die Angaben bereit, die dieser für sein eigenes Verzeichnis benötigt. Stellt er fest, dass von ihm verarbeitete Daten des Auftraggebers unrichtig oder veraltet sind, unterrichtet er den Auftraggeber unverzüglich.
- (3) Aufwand für Unterstützungsleistungen nach § 7 und diesem Paragraphen, der über das übliche Maß hinausgeht und nicht durch einen Verstoß des Auftragnehmers veranlasst ist, kann der Auftragnehmer nach vorheriger Ankündigung angemessen in Rechnung stellen.

§ 9 Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft, unverzüglich, spätestens innerhalb von 48 Stunden, nachdem sie ihm bekannt geworden ist, an die Adresse nach § 13. Die Meldepflicht besteht unabhängig davon, wie der Auftragnehmer das Risiko für die betroffenen Personen einschätzt; das Risiko bewertet der Auftraggeber, und er entscheidet über Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen.
- (2) Die Meldung enthält, soweit bereits bekannt, mindestens die Angaben nach Art. 33 Abs. 3 DSGVO:
 - a) eine Beschreibung der Verletzung einschließlich der betroffenen Kategorien von Daten und Personen sowie der ungefähren Zahl betroffener Personen und Datensätze,
 - b) Name und Kontaktdaten einer Anlaufstelle beim Auftragnehmer für weitere Informationen,
 - c) die voraussichtlichen Folgen der Verletzung,
 - d) die ergriffenen oder vorgeschlagenen Maßnahmen, um die Verletzung zu beheben und nachteilige Folgen abzumildern.
- (3) Fehlende Angaben reicht der Auftragnehmer unverzüglich nach, sobald sie vorliegen, und informiert den Auftraggeber über wesentliche neue Erkenntnisse.
- (4) Der Auftragnehmer ergreift unverzüglich die erforderlichen Maßnahmen, um die Verletzung einzudämmen und ihre Folgen zu mindern, dokumentiert die Verletzung und die ergriffenen Maßnahmen und unterstützt den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO.
- (5) Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen nimmt der Auftragnehmer für den Auftraggeber nur auf dessen Weisung vor. Eine Meldung nach Absatz 1 ist kein Anerkenntnis eines Verschuldens oder einer Haftung.

§ 10 Nachweise und Kontrollen

- (1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten nach Art. 28 DSGVO und nach dieser Vereinbarung nachzuweisen.
- (2) Der Auftraggeber kann die Einhaltung dieser Vereinbarung selbst oder durch einen von ihm beauftragten Prüfer überprüfen, der zur Verschwiegenheit verpflichtet ist und nicht im Wettbewerb mit dem Auftragnehmer steht. Überprüfungen umfassen auch Inspektionen in den Geschäftsräumen des Auftragnehmers; nach Absprache können sie aus der Ferne stattfinden, etwa per Videokonferenz.

Rechenzentren und Systeme der Unterauftragsverarbeiter werden anhand von deren Nachweisen überprüft, etwa Zertifikaten und Prüfberichten.

- (3) Inspektionen kündigt der Auftraggeber in der Regel mindestens 30 Tage vorher schriftlich oder in elektronischer Form an; bei begründetem Verdacht auf einen Verstoß genügt eine angemessene kürzere Frist. Sie finden zu den üblichen Geschäftszeiten statt, beeinträchtigen den Betrieb nicht unverhältnismäßig und wahren die Vertraulichkeit der Daten anderer Kunden und die Geschäftsgeheimnisse des Auftragnehmers.
- (4) Den Nachweis kann der Auftragnehmer vorrangig durch aktuelle Unterlagen erbringen, etwa die jeweils aktuelle Fassung der Anlagen 2 und 3, durch die Beantwortung von Fragenkatalogen sowie durch Zertifikate und Prüfberichte der Unterauftragsverarbeiter. Das Recht nach Absatz 2 bleibt unberührt.
- (5) Seinen Aufwand für Nachweise und Überprüfungen trägt der Auftragnehmer selbst, soweit er angemessen ist; angemessen ist jedenfalls ein Aufwand von bis zu einem Personentag je Kalenderjahr. Für darüber hinausgehenden Aufwand kann er nach vorheriger Ankündigung eine angemessene Vergütung verlangen, nicht jedoch, wenn die Überprüfung einen nicht nur unerheblichen Verstoß des Auftragnehmers gegen diese Vereinbarung ergibt.
- (6) Der Auftragnehmer arbeitet auf Anfrage mit der Aufsichtsbehörde zusammen (Art. 31 DSGVO). Er unterrichtet den Auftraggeber unverzüglich über Kontrollen, Anfragen und Maßnahmen einer Aufsichtsbehörde, soweit sie die Verarbeitung nach dieser Vereinbarung betreffen und eine Unterrichtung rechtlich zulässig ist. Der für den Auftraggeber zuständigen Aufsichtsbehörde stellt er auf Anfrage die Informationen nach diesem Paragraphen zur Verfügung.

§ 11 Löschung und Rückgabe

- (1) Über die Aufbewahrung der Inhalte, die der Auftraggeber und seine Benutzer in Feedcube anlegen oder erheben, insbesondere Umfragen, Antworten, Einladungen, Benutzerkonten und hochgeladene Dateien, entscheidet der Auftraggeber. Der Auftragnehmer speichert sie, bis der Auftraggeber sie in Feedcube löscht oder ihre Löschung anweist, längstens bis zur Löschung nach Absatz 4; während der Laufzeit des Hauptvertrags löscht er Inhalte nicht von sich aus. Personen mit der Rolle „Teilnehmer“ können ihr eigenes Benutzerkonto unter den Voraussetzungen der Anlage 1 Abschnitt 1 selbst löschen. Hochgeladene Dateien, die in Feedcube ersetzt oder entfernt werden oder deren zugehöriger Datensatz gelöscht wird, können bis zur Löschung nach Absatz 4 in der Dateiablage verbleiben; auf Weisung löscht der Auftragnehmer sie früher (Anlage 4 Abschnitt 2 Nr. 5). Technische Daten und Protokolle, einschließlich des Versandprotokolls der Einladungen (Anlage 4 Abschnitt 2 Nr. 8), löscht der Auftragnehmer nach den Fristen der Anlage 4.
- (2) Während der Laufzeit kann der Auftraggeber im Rahmen der von ihm vergebenen Berechtigungen Inhalte über die Funktionen von Feedcube löschen und Daten exportieren, etwa Antworten und Benutzerlisten; Exporte berücksichtigen die eingestellten Schwellen. Löschungen und Exporte, die über diese Funktionen nicht möglich sind, nimmt der Auftragnehmer auf Weisung des Auftraggebers vor.
- (3) Der Auftraggeber kann während der Laufzeit des Hauptvertrags und bis 30 Tage nach dessen Ende verlangen, dass der Auftragnehmer ihm die im Auftrag verarbeiteten personenbezogenen Daten in einem gängigen, maschinenlesbaren Format bereitstellt, auch wenn sein Zugang zu Feedcube eingeschränkt oder beendet ist. Der Auftragnehmer stellt die Daten innerhalb von 14 Tagen nach Zugang des Verlangens bereit.

- (4) Nach Ende des Hauptvertrags löscht der Auftragnehmer alle im Auftrag verarbeiteten personenbezogenen Daten einschließlich vorhandener Kopien spätestens 30 Tage nach Vertragsende, vorher nur auf Weisung des Auftraggebers; Absatz 5 und Anlage 4 Abschnitt 3 Abs. 2 bleiben unberührt. Ist eine fristgerecht verlangte Rückgabe zu diesem Zeitpunkt noch nicht abgeschlossen, löscht er die Daten unverzüglich nach ihrem Abschluss.
- (5) Daten in Datensicherungen, bei Unterauftragsverarbeitern und in Protokollen werden nach den Fristen der Anlage 4 gelöscht; Datensicherungen verwendet der Auftragnehmer bis dahin nur zur Wiederherstellung im Störfall. Daten aus Feedcube, die dem Auftragnehmer im Rahmen von Supportanfragen übermittelt wurden, löscht oder anonymisiert er, sobald sie für die Bearbeitung nicht mehr erforderlich sind, spätestens 24 Monate nach Abschluss der Anfrage und spätestens mit der Löschung nach Absatz 4 (Anlage 4 Abschnitt 2 Nr. 19).
- (6) Der Auftragnehmer bestätigt die Löschung auf Anforderung schriftlich oder in elektronischer Form. Ist er nach dem Recht der Union oder eines Mitgliedstaats verpflichtet, bestimmte Daten weiter zu speichern, teilt er dies dem Auftraggeber unter Angabe der Rechtsgrundlage mit, verarbeitet diese Daten nur noch für den gesetzlich vorgesehenen Zweck und wendet diese Vereinbarung bis zu ihrer Löschung weiter auf sie an.

§ 12 Haftung

- (1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO; diese Vereinbarung schränkt sie nicht ein.
- (2) Im Verhältnis der Parteien zueinander gelten die Haftungsregelungen des Hauptvertrags. Deren Beschränkungen und Ausschlüsse gelten nicht bei Vorsatz oder grober Fahrlässigkeit und nicht für Personenschäden.

§ 13 Ansprechpersonen

	Auftraggeber	Auftragnehmer
Weisungsberechtigt bzw. weisungsempfangsberechtigt	Name, Funktion, E-Mail:	Dominic Koch, office@feedcube.net
Ansprechperson Datenschutz	Name, E-Mail:	Dominic Koch, office@feedcube.net
Meldungen nach § 9	E-Mail, Telefon:	office@feedcube.net

Meldungen nach § 9 richtet der Auftragnehmer an die vom Auftraggeber angegebene Adresse; seine eigene Adresse ist die Anlaufstelle für Rückfragen zu Meldungen. Hat der Auftraggeber keine Angaben gemacht, gilt die Kontaktperson, die er bei Abschluss des Hauptvertrags angegeben hat, als weisungsberechtigt und als Empfängerin von Mitteilungen und Meldungen. Änderungen der Ansprechpersonen teilen sich die Parteien unverzüglich schriftlich oder in elektronischer Form mit.

§ 14 Schlussbestimmungen

- (1) In Fragen des Datenschutzes geht diese Vereinbarung dem Hauptvertrag und sonstigen Vereinbarungen der Parteien vor, soweit diese nicht ausdrücklich und in der Form nach Absatz 3 von ihr abweichen. Bei Widersprüchen innerhalb dieser Vereinbarung geht der Haupttext den Anlagen vor; im Übrigen geht die speziellere Regelung der allgemeineren vor.

- (2) Diese Vereinbarung ersetzt frühere Vereinbarungen der Parteien zur Auftragsverarbeitung für Feedcube, soweit die Parteien nichts anderes vereinbaren.
- (3) Änderungen und Ergänzungen dieser Vereinbarung einschließlich ihrer Anlagen bedürfen einer Vereinbarung in schriftlicher oder elektronischer Form. Ausgenommen sind die Anpassung der technischen und organisatorischen Maßnahmen nach § 5 Abs. 2, Änderungen bei den Unterauftragsverarbeitern nach § 6 und die Mitteilung geänderter Ansprechpersonen nach § 13. Wo diese Vereinbarung die schriftliche oder elektronische Form vorsieht, genügt eine E-Mail; einer Unterschrift bedarf es nicht.
- (4) Kann der Auftragnehmer Pflichten aus dieser Vereinbarung nicht erfüllen, teilt er dies dem Auftraggeber unverzüglich mit. Das Recht beider Parteien, den Hauptvertrag und diese Vereinbarung aus wichtigem Grund zu kündigen, bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragnehmer schwerwiegend gegen diese Vereinbarung verstößt und den Verstoß nicht innerhalb angemessener Frist behebt, oder wenn der Auftraggeber auf einer Weisung besteht, die nach begründeter Mitteilung des Auftragnehmers gegen Datenschutzrecht verstößt.
- (5) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine wirksame Regelung, die den Anforderungen des Art. 28 DSGVO entspricht und dem Zweck der unwirksamen Bestimmung am nächsten kommt.
- (6) Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts. Gerichtsstand ist das für 4224 Wartberg ob der Aist sachlich zuständige Gericht, sofern der Hauptvertrag nichts anderes bestimmt. Zwingende gesetzliche Gerichtsstände bleiben unberührt.

Anlagen

Die folgenden Anlagen sind Bestandteil dieser Vereinbarung:

- Anlage 1 – Beschreibung der Verarbeitung
- Anlage 2 – Technische und organisatorische Maßnahmen
- Anlage 3 – Unterauftragsverarbeiter
- Anlage 4 – Aufbewahrungs- und Löschfristen

Unterzeichnung

Eine Unterzeichnung ist nur erforderlich, wenn eine unterzeichnete Ausfertigung gewünscht wird (§ 1 Abs. 4).

Auftraggeber

Ort, Datum: _____

Unterschrift: _____

Name, Funktion: _____

Auftragnehmer

Ort, Datum: Wartberg ob der Aist, _____

Unterschrift: _____

Dominic Koch, Einzelunternehmer, Kochsoftware

Anlage 1 – Beschreibung der Verarbeitung

Stand: 11.10.2026

1. Gegenstand und Zweck

Der Auftragnehmer stellt dem Auftraggeber die Feedback- und Umfrageplattform Feedcube als Software-as-a-Service bereit und übernimmt dafür Betrieb, Hosting, Wartung und Support. Die Verarbeitung im Auftrag dient folgenden Zwecken:

- Erstellen, Versenden, Durchführen und Auswerten von Befragungen für die Einsatzzwecke, die der Auftraggeber festlegt, z. B. Kunden-, Kurs- und Seminar- oder Mitarbeitendenfeedback,
- zusammengefasste Auswertung der Antworten, etwa nach Umfragen, Zeiträumen, Fragen, Produkten, Standorten, Fachbereichen, Teams, Positionen oder Organisationseinheiten,
- Auswertung der Rückmeldungen zu einzelnen bewerteten Personen, z. B. Trainerinnen und Trainern oder Führungskräften; sie kann dem Auftraggeber als Grundlage für die Beurteilung der Leistung dieser Personen dienen, die KI-Funktionen sind dafür jedoch nicht bestimmt (Abschnitt 6 e),
- Verwaltung der Benutzerkonten, Rollen, Berechtigungen und der Organisationsstruktur des Auftraggebers,
- Betriebssicherheit, Datensicherung, Fehleranalyse und Support.

Gemeinsame Plattform. Feedcube läuft auf einer Plattform, die der Auftragnehmer auch für seine weiteren Produkte CourseMate, Quipla und Mindsketch nutzt (§ 1 Abs. 2 der Vereinbarung). Server, Server-Anwendung, Anmeldung und die Datenbank des Mandanten sind gemeinsam; ein Benutzerkonto im Mandanten des Auftraggebers gilt für alle Produkte der Plattform. Die weiteren Produkte sind nicht Gegenstand dieser Vereinbarung; bucht der Auftraggeber eines davon, gilt dafür eine gesonderte Ergänzung. Die weiteren Produkte sind im Mandanten auch ohne Buchung technisch erreichbar; was für Daten gilt, die dort dennoch verarbeitet werden, regelt § 1 Abs. 2 der Vereinbarung. Ein solches Produkt kann Daten aus Feedcube mitverwenden und nach eigenen Regeln anzeigen, etwa Benutzerkonten, Umfragen sowie Anzahl und Durchschnitt von Bewertungen, eigene Angaben zu Befragungen speichern, z. B. ob eine Person eine Befragung als erledigt markiert hat, und Daten in Feedcube anlegen, ändern oder löschen; so legt CourseMate Umfragen zu Seminaren an, nimmt Antworten über eine eigene Teilnehmerseite entgegen, versendet Teilnahmelinks per E-Mail und legt Benutzerkonten mit der Rolle „Teilnehmer“ an.

Aktivitätsprotokoll und Dateiablage des Mandanten sind für alle Produkte gemeinsam; Einträge der weiteren Produkte im Aktivitätsprotokoll können Namen und E-Mail-Adressen weiterer Personen enthalten. Die Einzelheiten regelt die jeweilige Ergänzung. Unabhängig von einer Buchung können Personen mit der Rolle „Teilnehmer“ ihr Benutzerkonto über die Profilfunktion von Quipla selbst löschen, sofern sie in Feedcube weder bewertet wurden noch Umfragen angelegt haben noch im Organigramm eingetragen sind; dabei entfallen auch ihre persönlichen Einladungen und ihre Zuordnungen zu Teams und Standorten.

2. Verarbeitungsvorgänge

Nr.	Vorgang	Beschreibung
1	Benutzerkonten, Rollen und Anmeldung	Anlegen, Ändern, Deaktivieren und Löschen von Benutzerkonten und Rollen, auch durch Import; Selbstregistrierung mit Bestätigung der E-Mail-Adresse, wobei selbst registrierte Personen erst Zugriff erhalten, wenn der Auftraggeber ihnen eine Rolle zuweist; Anmeldung mit Passwort, optional mit zweitem Faktor oder Passkey, mit Microsoft- oder Google-Konto oder per Single Sign-on über den Identitätsdienst des Auftraggebers, bei dessen Anbindung auch mit automatischer Anlage von Benutzerkonten in der vom Auftraggeber festgelegten Rolle; Zurücksetzen des Passworts; API-Schlüssel für die Programmierschnittstelle; Ansicht der Anwendung aus Sicht eines anderen Benutzerkontos durch Administratoren (Abschnitt 6 d)
2	Organisationsstruktur	Pflege von Teams, Positionen, Organigramm, Standorten und Fachbereichen und Zuordnung von Personen dazu; Grundlage für Empfängerkreise, Sichtbereiche und Auswertungseinheiten
3	Umfragen erstellen und verwalten	Anlegen und Pflegen von Fragen, Fragebögen, Vorlagen, Texten und Umfragen durch berechtigte Personen des Auftraggebers, auch über die Programmierschnittstelle mit persönlichen API-Schlüsseln; Anlegen von Umfragen aus Vorlagen auf Weisung des Auftraggebers auch mit dem Dienstschlüssel des Auftragnehmers (Anlage 2 Abschnitt 1); Zuordnung von Produkten, Standorten, Teams und bewerteten Personen; Festlegen von Zielgruppe und Gültigkeitszeitraum
4	Einladung zur Teilnahme	Versand von Einladungen per E-Mail mit persönlichem Teilnahmelink, einmalig an Personen mit Benutzerkonto oder nach Zeitplan an Personen mit Benutzerkonto und an weitere E-Mail-Adressen; alternativ ein offener Link oder QR-Code, den der Auftraggeber selbst verteilt; QR-Codes werden ohne Dienste Dritter erzeugt
5	Erhebung der Antworten	Speicherung der abgegebenen Antworten mit Abgabezeitpunkt und Angaben zur Umfrage, bei persönlich eingeladenen Personen mit Benutzerkonto zusätzlich mit Organisationsmerkmalen (Abschnitt 6 a)
6	Auswertung	Dashboards, Diagramme, Heatmap, Kommentarlisten, Zeitleisten, Einzelansichten, Berichte (PDF) und Export (CSV) für berechtigte Personen des Auftraggebers; Filter u. a. nach Zeitraum, Umfrage, Frage und Fragenkategorie, bewerteter Person, Produkt, Standort, Fachbereich, Team und Position; Auswertungen und Vergleiche je bewerteter Person, auch als Durchschnittsbewertung je Benutzerkonto in der Benutzerverwaltung; Organisations-Benchmark und Kennzahlen in Übersichten (Abschnitt 6 d)
7	KI-gestützte Auswertung und Übersetzung	Zusammenfassungen, Antworten auf frei formulierte Fragen, Berichte, Stimmungs- und Themenanalysen sowie KI-Zusammenfassung im PDF-Bericht; Übersetzung von Texten ins Englische, die berechtigte Personen in Feedcube pflegen; nur auf ausdrückliche Auslösung durch eine angemeldete Person mit der dafür erforderlichen Berechtigung und nur, solange der Auftraggeber die KI-Funktionen für seinen Mandanten nicht abgeschaltet hat (Abschnitt 6 e)
8	Benachrichtigungen	Systemnachrichten per E-Mail: Bestätigung der Selbstregistrierung, Zurücksetzen des Passworts, Hinweis mit Name und E-Mail-Adresse der neuen Person an alle Benutzerkonten mit der Rolle „Administrator“, auch deaktivierte, nach abgeschlossener Selbstregistrierung; Einladungen siehe Nr. 4

Nr.	Vorgang	Beschreibung
9	Protokollierung und Monitoring	Aktivitätsprotokoll der Anwendung, einsehbar für Personen mit der Berechtigung „Benutzer verwalten“; es lässt Rückschlüsse auf die Nutzung der Anwendung durch einzelne Personen zu. Zugriffsprotokolle der Webserver und Protokolle der Server-Anwendung; Aufzeichnung von Anmeldeversuchen, Selbstregistrierungen und Anfragen zum Zurücksetzen des Passworts zum Schutz vor Missbrauch; Fehler- und Leistungsmonitoring der Weboberfläche (Abschnitt 4, Anlage 3)
10	Datensicherung	Stündliche Sicherung der Datenbanken mit rollierender Aufbewahrung und Wiederherstellung im Störfall (Anlage 4)
11	Support	Bearbeitung von Supportanfragen des Auftraggebers; Daten aus Feedcube sieht der Auftragnehmer dabei nur ein, soweit es für die Bearbeitung erforderlich ist. Kontaktdaten der anfragenden Personen und die Kommunikation zur Anfrage verarbeitet er als Verantwortlicher (§ 1 Abs. 3 der Vereinbarung)
12	Dateiablage	Speicherung hochgeladener Bilder, z. B. Profil- und Teambilder, Firmenlogo und Hintergrundbilder von Umfragen
13	Löschung	Löschung durch den Auftraggeber in der Anwendung, durch Personen mit der Rolle „Teilnehmer“ für ihr eigenes Benutzerkonto (Abschnitt 1) oder durch den Auftragnehmer auf Weisung; täglicher automatischer Löschlauf für technische Daten und Protokolle in den Datenbanken, darunter das Versandprotokoll der Einladungen, und Rotation der Server-Protokolle nach den Fristen der Anlage 4; Inhalte des Auftraggebers löscht der Löschlauf nicht (Abschnitt 7)

3. Kategorien betroffener Personen

- Teilnehmende von Befragungen, je nach Einsatz z. B. Kundinnen und Kunden, Kurs- und Seminarteilnehmende oder Mitarbeitende des Auftraggebers,
- zu Befragungen eingeladene Personen, auch wenn sie nicht teilnehmen, einschließlich Empfängerinnen und Empfängern ohne Benutzerkonto,
- Personen, die in Befragungen bewertet werden, z. B. Trainerinnen und Trainer, Führungskräfte oder andere Mitarbeitende, sowie Personen, die in Fragen oder Antworten genannt werden,
- Personen mit Benutzerkonto im Mandanten des Auftraggebers, z. B. für Administration, Umfrageverwaltung und Auswertung, einschließlich Personen, die sich selbst registrieren,
- Personen, die Seiten von Feedcube aufrufen, etwa zur Anmeldung, zur Registrierung oder zum Zurücksetzen des Passworts, oder die einen Teilnahmelink öffnen.

4. Arten personenbezogener Daten

Datenart	Inhalt
Kontodaten	Vorname, Nachname, E-Mail-Adresse, Rolle, Kontostatus (aktiv oder deaktiviert), Zeitpunkt der Anlage, optional Profilbild; bei Selbstregistrierung bis zur Bestätigung Name, E-Mail-Adresse, Passwort-Hash und Bestätigungscode (als Hash)
Organisationsdaten	Zuordnung zu Teams, Positionen, Standorten und Fachbereichen; Stelle im Organigramm einschließlich der übergeordneten Person

Datenart	Inhalt
Authentifizierungsdaten	Passwort (nur als Einweg-Hash); Code zum Zurücksetzen des Passworts (als Hash) mit Zeitpunkt; Merkmale des zweiten Faktors und Passkeys; API-Schlüssel (als Einweg-Hash) mit Bezeichnung, Anfangszeichen und den Zeitpunkten von Erstellung, Ablauf und letzter Nutzung; Sitzungs-Token (als Hash) mit IP-Adresse und Browser-Kennung; IP-Adresse und eingegebene E-Mail-Adresse bei Anmeldeversuchen, Selbstregistrierungen und Anfragen zum Zurücksetzen des Passworts; IP-Adresse bei der Abfrage des zweiten Faktors; Kennung des Benutzerkontos bei Fehlversuchen beim Bestätigen des aktuellen Passworts; bei Anmeldung über Microsoft, Google oder den Identitätsdienst des Auftraggebers die dabei übermittelten Angaben, insbesondere E-Mail-Adresse, Name und Kennung des Kontos; bei Anbindung des Identitätsdienstes des Auftraggebers die Angaben nach Anlage 3 Abschnitt 2 Abs. 1
Umfragedaten	Fragen und Texte, Zielgruppe, Gültigkeitszeitraum, zugeordnete Produkte, Standorte und Teams, zugeordnete bewertete Personen mit Name und gegebenenfalls Profilbild, anlegende Person
Einladungsdaten	E-Mail-Adresse und Name der eingeladenen Person bzw. ihr Benutzerkonto, persönlicher Teilnahmelink mit dem Zeitpunkt seiner Erzeugung, Betreff und Inhalt der Einladung, Zeitplan; Versandprotokoll mit Name und E-Mail-Adresse der Empfängerin oder des Empfängers, Betreff, Inhalt (beim Versand nach Zeitplan einschließlich des persönlichen Teilnahmelinks), Versandzeitpunkt, Versandstatus und bei fehlgeschlagenem Versand nach Zeitplan der Fehlermeldung
Antwortdaten	Skalenwerte, Auswahlantworten, Freitexte, Datum und Uhrzeit der Abgabe, zugehörige Umfrage; bei persönlich eingeladenen Personen mit Benutzerkonto zusätzlich Team, Position und Organisationseinheit zum Zeitpunkt der Abgabe (Abschnitt 6 a)
Bezugsdaten der Bewertung	bei Umfragen mit bewerteten Personen die bewertete Person; je nach Umfrage Produkt oder Thema mit Produktnummer (z. B. Kursnummer), Standort, Fachbereich und Zielgruppe
Protokolldaten	Aktivitätsprotokoll mit Ereignis (z. B. Anmeldung, Änderung, Löschung, Export der Benutzerliste, Auslösung einer KI-Funktion), gegebenenfalls mit interner Kennung oder Bezeichnung des betroffenen Objekts, Zeitpunkt und E-Mail-Adresse des handelnden Benutzerkontos, bei Anmelde- und Registrierungsversuchen der eingegebenen E-Mail-Adresse und bei der Ansicht als anderer Benutzer zusätzlich der E-Mail-Adresse des angesehenen Kontos; das Aktivitätsprotokoll ist für alle Produkte der Plattform gemeinsam (Abschnitt 1); Zugriffsprotokolle der Webserver mit IP-Adresse, Zeitpunkt, aufgerufener Adresse, die deren Parameter enthalten kann (z. B. Teilnahmelinks, Codes aus Registrierungs- und Passwort-Links, E-Mail-Adressen, Filtereinstellungen, frei formulierte Fragen an die KI-gestützte Auswertung), Statuscode, Herkunftsadresse (bei Anfragen der Weboberfläche die Adresse der aufrufenden Seite) und gegebenenfalls Browser-Kennung; Protokolle der Server-Anwendung, nämlich ein Zugriffsprotokoll mit IP-Adresse, Zeitpunkt, aufgerufener Adresse und Statuscode, in dem Parameterwerte, E-Mail-Adressen und tokenartige Bestandteile der Adresse durch Platzhalter ersetzt sind, sowie Betriebs- und Fehlermeldungen; Meldungen, die Feedcube selbst schreibt, enthalten keine Namen oder E-Mail-Adressen, Fehlerberichte zu unbehandelten Fehlern werden um erkannte E-Mail-Adressen und Token bereinigt, Meldungen der weiteren Produkte der Plattform können dagegen E-Mail-Adressen und weitere Angaben enthalten (Anlage 2 Abschnitt 2)

Datenart	Inhalt
Technische Nutzungsdaten (Monitoring)	erfasst in der Weboberfläche, nicht jedoch auf der Teilnehmerseite und auf den Seiten für Anmeldung, Registrierung, Passwort, Zwei-Faktor-Abfrage, Single Sign-on, Freischaltung und Auswahl der Organisation: IP-Adresse und gegebenenfalls ein daraus abgeleiteter ungefährender Standort (Land, Ort), Browser- und Geräteangaben, aufgerufene Seiten- und Schnittstellenadressen ohne Abfrageparameter (E-Mail-Adressen und tokenartige Bestandteile werden vor der Übermittlung ersetzt), Bedienschritte ohne den Text des angeklickten Elements, Lade- und Antwortzeiten, Fehlermeldungen (in Meldungstext und Stacktrace werden erkannte E-Mail-Adressen, Token und Zugangsdaten ersetzt; Fehlertexte können dennoch Namen oder andere Inhalte enthalten); bei angemeldeten Personen verknüpft mit ihrer internen Benutzerkennung, nicht mit Name oder E-Mail-Adresse; ohne Aufzeichnung von Sitzungen und ohne Speicherung im Browser
Daten im Browser	Bei angemeldeten Personen legt die Weboberfläche technisch erforderliche Cookies für die Sitzung und den Schutz vor Cross-Site-Request-Forgery sowie Cookies mit Anzeigeeinstellungen der Seitenleiste ab; ist der zentrale Anmeldedienst für den Mandanten eingerichtet (Anlage 3 Abschnitt 3 Abs. 1), setzt dieser ein Cookie für die Anmeldesitzung. Bei der Anmeldung mit Microsoft legt dessen Anmeldebibliothek bis zum Abschluss der Anmeldung eigene Cookies, Kontoangaben und Token im Browser ab; die Weboberfläche entfernt sie danach. Im lokalen Speicher und im Sitzungsspeicher des Browsers können Angaben wie Name, E-Mail-Adresse, Rolle und Berechtigungen sowie Anzeigeeinstellungen liegen, im Sitzungsspeicher des jeweiligen Browser-Tabs auch Zwischenstände beim Anlegen von Einladungen und während der Ansicht als anderer Benutzer (Abschnitt 6 d) deren Zugriffstoken mit Name, E-Mail-Adresse, Rolle und Berechtigungen der angesehenen Person. Bei der Abmeldung entfernt die Weboberfläche die personen- und sitzungsbezogenen Angaben aus dem Browser, und der Server löscht die Cookies für Sitzung und Schutz vor Cross-Site-Request-Forgery. Nach automatischer Abmeldung, Ablauf oder Beendigung der Sitzung und nach Deaktivierung des Kontos entfernt die Weboberfläche diese Angaben, sobald sie das bei geöffneter Weboberfläche feststellt, andernfalls beim nächsten Aufruf der Weboberfläche in diesem Browser; die Cookies verbleiben bis zu ihrem Ablauf, sind auf dem Server dann aber ungültig. Anzeigeeinstellungen und technische Angaben ohne Personenbezug, etwa die gewählte Organisation, bleiben erhalten und können auch vor der Anmeldung gespeichert werden. Die Teilnehmerseite setzt keine Cookies; sie entfernt das Kennzeichen des Teilnahmelinks aus der Adresszeile und hält es nur im Sitzungsspeicher des Browser-Tabs. Mit dem Schließen des Tabs entfällt es, sofern der Browser den Tab nicht wiederherstellt; die Teilnehmerseite, auf die die Teilnahmelinks von Feedcube führen, löscht es bereits nach erfolgreicher Abgabe sowie bei abgelaufener, noch nicht begonnener oder unbekannter Umfrage. Im Verlauf des Browsers bleibt der ursprüngliche Link erhalten.
Dateien	hochgeladene Bilder, z. B. Profil- und Teambilder, Firmenlogo und Hintergrundbilder; vorübergehend auf dem Server erzeugte Exportdateien mit Antwortdaten (Anlage 4 Abschnitt 2 Nr. 7)
Supportdaten	Daten aus Feedcube, die eine Supportanfrage enthält oder die bei ihrer Bearbeitung eingesehen werden; technische Diagnosedaten

5. Besondere Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) und von Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) ist nicht Gegenstand des Auftrags. Da Teilnehmende in Freitextfeldern beliebige Inhalte eingeben können, lässt sich das Vorkommen solcher Daten technisch nicht ausschließen; gehen sie ein, behandelt der Auftragnehmer sie wie alle übrigen Antwortdaten nach dieser Vereinbarung. Der Auftraggeber gestaltet Fragen und Hinweise an die Teilnehmenden so, dass solche Angaben nicht abgefragt werden. Sollen sie ausnahmsweise erhoben werden, etwa mit Fragen zur gesundheitlichen Belastung, stimmt er dies vorher mit dem Auftragnehmer ab.

6. Schutzvorkehrungen bei Befragungen und Auswertungen und ihre Grenzen

Dieser Abschnitt beschreibt, welche Angaben Feedcube zu Antworten speichert und anzeigt, wie der Auftraggeber die Einsicht steuert und wo die Vorkehrungen an Grenzen stoßen. Ob sich Antworten einzelnen Personen zuordnen lassen, hängt auch von der Gestaltung der Befragung durch den Auftraggeber ab, insbesondere von Fragen und Freitexten, der Größe der befragten Gruppen und den eingestellten Schuttschwellen.

- a) **Angaben zu einer Antwort.** Feedcube speichert eine Antwort ohne Benutzerkennung, E-Mail-Adresse und IP-Adresse der antwortenden Person, aber mit Datum und Uhrzeit der Abgabe. Lädt der Auftraggeber eine Person über ihr Benutzerkonto im Mandanten mit einem persönlichen Teilnahmelink ein und ist das Konto bei der Abgabe aktiv und freigeschaltet, übernimmt Feedcube bei der Abgabe zusätzlich Team, Position und Organisationseinheit dieses Kontos, soweit diese hinterlegt sind (Organisationsmerkmale); Organisationseinheit ist dabei die Gruppe der Personen, die im Organigramm derselben übergeordneten Person zugeordnet sind. Wird eine Person nur über ihre E-Mail-Adresse eingeladen, auch wenn ein Benutzerkonto mit dieser Adresse besteht, oder ist ihr Konto deaktiviert oder nicht freigeschaltet, speichert Feedcube die Antwort ohne Organisationsmerkmale. In kleinen Einheiten kann die Kombination dieser Merkmale auf eine einzelne Person hinweisen; solche Antworten können dann einer Person zugeordnet werden und sind insoweit nicht anonym. Dem wirken die Schuttschwellen nach Buchstabe c entgegen. Eine Antwort mit Organisationsmerkmalen lässt außerdem erkennen, dass sie über einen persönlichen Teilnahmelink abgegeben wurde.
- Ob oder wann eine eingeladene Person ihren persönlichen Teilnahmelink geöffnet oder eine Antwort abgegeben hat, vermerkt Feedcube in den Einladungsdaten nicht; Einladungen nach Zeitplan gehen deshalb bei jedem Versand an alle Empfängerinnen und Empfänger, unabhängig davon, ob sie bereits geantwortet haben; ausgenommen sind deaktivierte und nicht freigeschaltete Konten, und mit dem Ende der Umfrage endet der Versand. Beim Versand der E-Mails ist die Erfassung von Öffnungen und Klicks durch den Versanddienst abgeschaltet. Weitere Produkte können eigene Angaben dazu speichern, etwa CourseMate, ob und wann eine Person eine Befragung als erledigt markiert hat (Abschnitt 1).
 - Die Webserver und die Server-Anwendung protokollieren Aufrufe mit IP-Adresse, Zeitpunkt und aufgerufener Adresse. Die Server-Anwendung ersetzt in ihrem Zugriffsprotokoll die Werte von Adressparametern und damit auch das Kennzeichen persönlicher Teilnahmelinks; in den Zugriffsprotokollen der Webserver kann die protokollierte Adresse das Kennzeichen dagegen enthalten. Für die Dauer der Aufbewahrung dieser Protokolle von 14 Tagen (Anlage 4 Abschnitt 2 Nr. 14) ließe sich darüber feststellen, ob und wann ein persönlicher Teilnahmelink aufgerufen wurde, und zusammen mit dem Abgabezeitpunkt eine Antwort der eingeladenen Person zuordnen. Der Auftragnehmer verwendet diese Protokolle nur zu den in Anlage 4 Abschnitt 2 Abs. 4 genannten Zwecken und wertet sie nicht aus, um Teilnahmen oder Antworten einzelnen Personen zuzuordnen; in der Anwendung sind sie nicht einsehbar.
 - Macht eine Person Angaben zu ihrer Antwort, etwa zum Zeitpunkt der Abgabe und zum Wortlaut, lässt sich eine nicht geschützte Antwort in der Anwendung über Filter, etwa nach Zeitraum und Antwortinhalt, auffinden und von Personen mit der Berechtigung „Feedback löschen“ löschen, soweit sie in deren Sichtbereich liegt (Buchstabe d). Gelöscht wird jeweils der Datensatz zu einer bewerteten Person; betrifft eine Abgabe mehrere bewertete Personen, ist jeder Datensatz zu löschen. Geschützte Antworten (Buchstabe c) zeigt Feedcube ohne Wortlaut und Zeitpunkt; um eine solche Antwort aufzufinden, kann der Auftraggeber den Auftragnehmer anweisen, sie herauszusuchen. Schaltet er stattdessen die Schuttschwelle vorübergehend aus, werden für diese Zeit alle bisher geschützten Antworten im Rahmen der Sichtbereiche sichtbar.

- b) **Befragung über offenen Link oder QR-Code.** Antworten über einen offenen Link oder QR-Code speichert Feedcube ohne Organisationsmerkmale; Einladungsdaten entstehen dabei in Feedcube nicht. Jede Person, die einen offenen Link kennt, kann ihn innerhalb des Gültigkeitszeitraums der Umfrage mehrfach verwenden. In der Auswertung schützt solche Antworten nur die Mindestanzahl je Umfrage nach Buchstabe c.
- Ist einer Umfrage eine bewertete Person zugeordnet, zeigt die Teilnehmerseite deren Namen an; bei offenen Links und QR-Codes kann ihn jede Person sehen, die den Link kennt. Der Abruf der Umfrage über den Teilnahmelink liefert die für die Anzeige des Fragebogens erforderlichen Angaben und wenige technische Angaben wie die internen Kennungen der Fragen, aber keine Kennungen von Benutzerkonten oder anderen Teilnahmelinks; vor Beginn und nach Ende des Gültigkeitszeitraums liefert er weder Fragen noch Namen. Fragetexte und allgemeine Einstellungen des Mandanten, etwa Farben, Logo und Bezeichnungen, lädt die Teilnehmerseite über weitere ohne Anmeldung erreichbare Schnittstellen, die keine Namen oder Kennungen von Personen liefern. Fragetexte sind darüber anhand ihrer Kennung auch unabhängig von einem Teilnahmelink und vom Gültigkeitszeitraum abrufbar; sie sollten daher keine vertraulichen Angaben enthalten.
 - Abgaben vor Beginn oder nach Ende des Gültigkeitszeitraums einer Umfrage weist Feedcube auf dem Server zurück und speichert sie nicht.
- c) **Anonymitätsschutz in der Auswertung.** Feedcube bietet zwei Schwellen. Sie gelten für alle Umfragen des Mandanten, auch für bereits bestehende, und zwar in Dashboard, Diagrammen, Heatmap, Kommentarlisten, Berichten, Export und KI-gestützter Auswertung:
- *Mindestgröße der Personengruppe:* Feedcube zeigt eine Auswertung nicht an, wenn sich die einbezogenen Antworten mit Organisationsmerkmalen – etwa nach dem Filtern auf ein Team oder eine Position – auf weniger mögliche Absenderinnen und Absender zurückführen lassen als eingestellt. Einzelne Antworten aus zu kleinen Personengruppen schützt Feedcube auch innerhalb größerer Auswertungen. Als mögliche Absenderinnen und Absender zählen die Personen mit denselben Organisationsmerkmalen nach der Organisationsstruktur zum Zeitpunkt der Auswertung, nicht der Kreis der Eingeladenen; wer die Empfängerliste einer Umfrage kennt, kann den Kreis daher unter Umständen enger eingrenzen. Deaktivierte Benutzerkonten zählen nicht mit, nicht freigeschaltete dagegen schon, obwohl Abgaben über deren persönliche Teilnahmelinks ohne Organisationsmerkmale gespeichert werden; gehört einer Kombination von Organisationsmerkmalen zum Zeitpunkt der Auswertung niemand mehr an, bleiben die betreffenden Antworten geschützt. Änderungen der Organisationsstruktur, etwa Versetzungen, Zu- und Abgänge oder aufgelöste Teams, können nachträglich verändern, ob eine Antwort geschützt ist, und den Schutz auch aufheben. Antworten ohne Organisationsmerkmale, etwa über offene Links, QR-Codes, Einladungen an E-Mail-Adressen statt an Benutzerkonten oder über persönliche Teilnahmelinks deaktivierter oder nicht freigeschalteter Konten, erfasst diese Schwelle nicht.
 - *Mindestanzahl abgegebener Antworten je Umfrage:* Solange eine Umfrage weniger Antworten erhalten hat als eingestellt, sind alle ihre Antworten geschützt. Gezählt werden die Abgaben zu der Umfrage, die mindestens eine Antwort enthalten; eine Abgabe, die mehrere bewertete Personen betrifft, zählt einmal. Da offene und persönliche Teilnahmelinks mehrfach verwendet werden können, tragen auch wiederholte Abgaben über dieselben Links zur Mindestanzahl bei.
 - *Wirkung:* Werte und Texte geschützter Antworten fließen in keine angezeigte Durchschnitts-, Verteilungs- oder Textauswertung, keinen Export und keine KI-gestützte Auswertung ein. Erkennbar bleibt, dass sie abgegeben wurden: Sie zählen in Anzahlen mit und erscheinen in Listen als Einträge mit dem Hinweis „Geschützt“; je nach Ansicht bleiben dabei Umfrage, Produkt, Standort, Frage und gegebenenfalls die bewertete Person sichtbar. Team und Abgabezeitpunkt einer geschützten Antwort zeigt Feedcube weder in Listen und Einzelansichten noch im Export an. Filter nach Zeitraum, Team und Position wirken jedoch

auch auf geschützte Antworten: Wer so filtert und Anzahlen oder Listeneinträge vergleicht, kann unter Umständen ableiten, an welchem Tag eine geschützte Antwort abgegeben wurde und welchem Team oder welcher Position sie zuzuordnen ist. Ein Filter nach der Antwort auf eine bestimmte Frage berücksichtigt geschützte Antworten dagegen nicht. Vollständig blendet Feedcube eine Auswertung aus, wenn alle einbezogenen Antworten geschützt sind oder wenn die einbezogenen Antworten mit Organisationsmerkmalen insgesamt auf weniger mögliche Absenderinnen und Absender zurückgehen als eingestellt; im zweiten Fall zeigt Feedcube auch die einbezogenen Antworten ohne Organisationsmerkmale nicht an.

- *Einstellung:* Ein Wert von 0 schaltet die jeweilige Schwelle aus. In neu eingerichteten Mandanten sind beide Schwellen auf 5 voreingestellt; in früher eingerichteten Mandanten können sie ausgeschaltet sein. Der Auftraggeber schaltet die Schwellen unter „Einstellungen“, Reiter „Feedcube“, Bereich „Anonymität der Auswertung“ mit den Schaltern „Anonymitätsschutz aktivieren“ und „Mindestanzahl Bewertungen pro Umfrage aktivieren“ ein und legt dort die Werte fest; dort ist auch ersichtlich, welche Werte gelten. Ändern kann sie nur, wer die Berechtigung „Look & Feel“ hat. Diese Berechtigung können Personen mit der Administratorrolle vergeben sowie Personen mit den Berechtigungen „Rollen verwalten“ oder „Benutzer verwalten“, deren eigene Rolle sie enthält; wer die Berechtigung „Integrationen verwalten“ hat, legt außerdem die Rolle von Konten fest, die bei angebundenem Identitätsdienst automatisch angelegt werden (Anlage 2 Abschnitt 1, Zugriffskontrolle). Dieselbe Berechtigung steuert den Organisations-Benchmark (Buchstabe d), die Freigabe der KI-Funktionen (Buchstabe e) und die Sichtbarkeit der Module; wird das Modul „Standorte“ ausgeblendet, entfällt die Begrenzung der Sichtbereiche auf Standorte.
 - *Empfehlung:* Sichert der Auftraggeber den Teilnehmenden Anonymität zu oder wertet er nach Teams, Positionen oder Organisationseinheiten aus, empfiehlt der Auftragnehmer, beide Schwellen auf jeweils mindestens 5 zu setzen, unabhängig von einem Wert, den die Oberfläche beim Einschalten vorschlägt, und die Berechtigungen „Look & Feel“, „Rollen verwalten“, „Benutzer verwalten“ und „Integrationen verwalten“ nur Personen zu erteilen, die über diese Einstellungen entscheiden sollen. Auf Weisung des Auftraggebers stellt der Auftragnehmer die Werte ein.
- d) **Sichtbereiche.** Welche Antworten in die Auswertungen einer angemeldeten Person einfließen, richtet sich nach den Berechtigungen, die der Auftraggeber ihrer Rolle erteilt (Sichtbereich). Dafür gelten die folgenden Regeln und Ausnahmen:
- Ohne weitere Berechtigung umfasst der Sichtbereich nur Feedback, in dem die Person selbst bewertet wurde. Dieses Feedback ist ihr technisch auch dann zugänglich, wenn ihr die Berechtigung „Eigenes Feedback auswerten“ fehlt, sofern ihre Rolle eine andere Auswertungs- oder Verwaltungsberechtigung von Feedcube enthält. Konten ohne eine solche Berechtigung, etwa mit der Standardrolle „Teilnehmer“, erhalten keine Auswertungen.
 - „Eigenes Team Feedback auswerten“ erweitert den Sichtbereich auf Feedback, in dem Mitglieder der eigenen Teams bewertet wurden, und auf Antworten ohne bewertete Person, die Mitglieder dieser Teams über persönliche Teilnahmelinks abgegeben haben; „Feedback unterstellter Mitarbeiter:innen auswerten“ entsprechend auf Feedback zu Personen unterhalb der Person im Organigramm und auf Antworten ohne bewertete Person aus Organisationseinheiten unterhalb der Person, sofern diese selbst im Organigramm eingetragen ist; „Organisations-unabhängig Feedback auswerten“ auf alle Antworten des Mandanten.
 - Ohne „Standort-übergreifend“ bzw. „Fachbereichs-übergreifend“ bleibt der Sichtbereich auf die der Person zugeordneten Standorte bzw. Fachbereiche begrenzt; ist ihr keiner zugeordnet, umfasst er insoweit kein Feedback. Ist das Modul „Standorte“ ausgeblendet, entfällt die Begrenzung auf Standorte.
 - *Ausnahme Organisations-Benchmark:* Die Kennzahl „Ø Organisation“, die Vergleichskurve und die Radar-Serie „Organisation gesamt“ im Dashboard zeigen Durchschnittswerte über alle Antworten des Mandanten im gewählten Zeitraum und gegebenenfalls in der gewählten Zielgruppe, ohne

Aufschlüsselung nach Personen oder Organisationseinheiten. Sie stehen allen angemeldeten Personen des Mandanten zur Verfügung, deren Rolle eine Auswertungs- oder Verwaltungsberechtigung von Feedcube enthält, unabhängig von ihrem Sichtbereich. Feedcube zeigt einen solchen Wert nur, wenn ihm mindestens fünf nicht geschützte Abgaben mit Bewertungen zugrunde liegen, bei einer höher eingestellten Mindestanzahl je Umfrage (Buchstabe c) mindestens so viele; das gilt auch für jeden Punkt der Vergleichskurve und jeden Wert der Radar-Serie. Rückschlüsse auf einzelne Bewertungen außerhalb des eigenen Sichtbereichs lassen sich dadurch erschweren, aber nicht in jedem Fall ausschließen, etwa durch den Vergleich der Werte zweier kurz aufeinanderfolgender Zeiträume. Geschützte Antworten (Buchstabe c) fließen nicht ein. Der Benchmark ist voreingestellt eingeschaltet und lässt sich unter „Einstellungen“, Reiter „Feedcube“, Bereich „Dashboard“ mit dem Schalter „Organisations-Benchmark“ für den Mandanten abschalten.

- *Ausnahme Umfragenliste:* Personen mit der Berechtigung „Umfragen verwalten“ sehen in der Umfragenliste ohne gesetzte Filter zu den dort angezeigten Umfragen die Anzahl der Antworten und die Durchschnittsbewertung über alle Antworten der jeweiligen Umfrage, auch soweit diese außerhalb ihres Sichtbereichs liegen; geschützte Werte fließen in den Durchschnitt nicht ein.
 - *Ausnahme Anzahlen:* In einzelnen Übersichten, etwa bei den Standorten, kann die Anzahl der Antworten auch über den Sichtbereich hinaus angezeigt werden.
 - *Ansicht als anderer Benutzer:* Personen mit der Administratorrolle können in der Benutzerverwaltung über „Als diese Person ansehen“ die Anwendung aus Sicht eines anderen aktiven Benutzerkontos aufrufen, das nicht die Administratorrolle hat, jeweils für höchstens 30 Minuten. Sie sehen dabei, was diese Person sehen darf, einschließlich ihrer persönlichen Angaben. Änderungen sind in dieser Ansicht nicht möglich, KI-gestützte Auswertungen können jedoch ausgelöst werden. Der Beginn der Ansicht wird im Aktivitätsprotokoll vermerkt. Lesende Handlungen in der Ansicht, etwa ein Export der Benutzerliste, können dort unter dem Benutzerkonto der angesehenen Person vermerkt sein; ausgelöste KI-Auswertungen werden unter dem Benutzerkonto des Administrators mit Hinweis auf die Ansicht vermerkt.
 - *Stammdaten:* Die Sichtbereiche begrenzen Antworten und Auswertungen. Namen, Rollen und Profilbilder der Benutzerkonten sowie die Teamzugehörigkeit von Personen können alle angemeldeten Personen des Mandanten abrufen, auch Konten mit der Rolle „Teilnehmer“. Personen mit einer Auswertungs-berechtigung erhalten für die Filter der Auswertungen außerdem die Bezeichnungen von Produkten, Standorten, Fachbereichen, Fragenkategorien, Fragen, Teams und Positionen sowie den Zeitpunkt der ältesten Antwort des Mandanten; die Übersicht der Umfragen mit Produkt, Produktnummer, Standort, Datum der Anlage sowie Name und Profilbild der Person, die die Umfrage angelegt hat oder der sie zugeordnet ist, die Produktnummern und die bewerteten Personen stammen dabei aus den Antworten ihres Sichtbereichs. Teilnahmelinks sehen Personen mit der Berechtigung „Umfragen verwalten“ und je nach Rolle auch weitere Personen, etwa für Umfragen mit Feedback in ihrem Sichtbereich. Je nach Rolle können über Funktionen der gemeinsamen Plattform auch die E-Mail-Adressen anderer Benutzerkonten abrufbar sein.
 - *Andere Produkte:* Zeigen andere Produkte der Plattform Daten aus Feedcube an, gelten dafür deren Regeln (Abschnitt 1).
- e) **KI-gestützte Auswertung und Übersetzung.** KI-Funktionen laufen nicht selbsttätig, weder zeitgesteuert noch im Hintergrund. Sie werden nur ausgeführt, wenn eine angemeldete Person des Auftraggebers sie ausdrücklich anfordert, in der Weboberfläche insbesondere über „KI-Analyse“ in den Kommentarlisten (z. B. im Dashboard, auf der Seite „Kommentare“ und in der Auswertung einer Umfrage, Frage oder Kategorie) für eine Zusammenfassung, eine frei formulierte Frage oder einen Bericht, über die Stimmungs- oder Themenanalyse auf der Seite „Kommentare“ oder mit der Wahl „Mit KI-Zusammenfassung“ beim Erstellen eines PDF-Berichts. Anfragen mit einem API-Schlüssel weist Feedcube

für die KI-Funktionen zurück. Die KI-Zusammenfassung für einen PDF-Bericht wird vor der Übernahme zur Prüfung angezeigt und kann dort bearbeitet werden; der PDF-Bericht enthält nur den dort bestätigten Text. Wird das Textfeld dabei vollständig geleert, enthält er keine KI-Zusammenfassung; ein neuer KI-Aufruf erfolgt dabei nicht. Schlägt die Erstellung der KI-Zusammenfassung fehl, stellt Feedcube keine Ersatzanfrage. Den Bericht der KI-Analyse (HTML) erstellt Feedcube dagegen in einem Schritt ohne Prüfdialog und weist darauf hin, dass sein Inhalt zu prüfen ist. Die Zahl der KI-Anfragen je Benutzerkonto ist begrenzt.

- *Freigabe im Mandanten:* Der Auftraggeber legt unter „Einstellungen“, Reiter „Feedcube“, Bereich „KI-Funktionen“ mit dem Schalter „KI-Funktionen erlauben“ fest, ob die KI-Funktionen von Feedcube in seinem Mandanten genutzt werden dürfen; ändern kann den Schalter, wer die Berechtigung „Look & Feel“ hat. Ist er ausgeschaltet, bietet Feedcube die KI-Funktionen nicht an, weist entsprechende Anfragen zurück, ohne Daten zu lesen, und übermittelt aus Feedcube nichts an die KI-Dienste, auch nicht für die Übersetzung; die gemeinsame Übersetzungsfunktion der Plattform ist dann auch in den weiteren Produkten gesperrt. In neu eingerichteten Mandanten ist der Schalter voreingestellt ausgeschaltet; in Mandanten, die vor Einführung des Schalters eingerichtet wurden, ist er eingeschaltet, bis der Auftraggeber ihn ausschaltet. Die übrigen KI-Funktionen von Quipla und Mindsketch erfasst der Schalter nicht; für sie gelten deren Ergänzungen (§ 1 Abs. 2 der Vereinbarung).
- *Zweckbestimmung:* Die KI-Funktionen unterstützen Personen des Auftraggebers beim Auswerten von Befragungen, etwa zur Verbesserung von Angeboten, Kursen, Dienstleistungen und Abläufen, und beim Übersetzen von Texten, die sie in Feedcube pflegen. Sie sind nicht dazu bestimmt, Entscheidungen über einzelne Personen zu treffen oder vorzubereiten oder Leistung oder Verhalten einzelner Personen in einem Beschäftigungs- oder Auftragsverhältnis zu beurteilen. Setzt der Auftraggeber sie dafür ein, kann er nach Art. 25 Abs. 1 lit. c der Verordnung (EU) 2024/1689 selbst die Pflichten eines Anbieters eines Hochrisiko-KI-Systems tragen. Bei Umfragen mit bewerteten Personen übermittelt Feedcube je nach Funktion zu jeder Antwort einen Platzhalter der bewerteten Person, die Themenanalyse kennt das Thema „Trainer-Kompetenz“, und die Ergebnislisten von Stimmungs- und Themenanalyse nennen zu jedem Kommentar die bewertete Person; KI-Ergebnisse können sich daher auf einzelne Personen beziehen (§ 3 Abs. 2 lit. e der Vereinbarung).
- *Übermittelte Daten:* Übermittelt werden Antworten aus der gewählten Auswahl im Sichtbereich der auslösenden Person, je nach Funktion bis zu 500 Freitextantworten sowie Kennzahlen und Verteilungen der Bewertungen, außerdem die Beschreibung der gesetzten Filter einschließlich eines gewählten Zeitraums und gegebenenfalls die frei formulierte Frage. Je nach Funktion werden als Kontextangaben Fragetext, Bezeichnungen von Produkt, Standort, Fragenkategorie und Bewertungsstufen, die häufigste Antwort je Auswahlfrage und der Monat der Abgabe mitgesendet, bei Umfragen mit bewerteten Personen statt deren Namen ein Platzhalter. Produktnummer, Zielgruppe, Fachbereich, Tag und Uhrzeit der Abgabe sowie interne Kennungen von Umfragen und Benutzerkonten übermittelt Feedcube nicht; ein eng gewählter Zeitraum in der Filterbeschreibung kann jedoch den Tag der Abgabe erkennen lassen. Stimmungs- und Themenanalyse übermitteln nur die Kommentartexte. Bei den Auswertungsfunktionen wird jede Antwort vor der Übermittlung auf höchstens 2.000 Zeichen gekürzt. Antworten und Kennzahlen übergibt Feedcube getrennt von den Anweisungen an das Sprachmodell in einem gekennzeichneten Datenblock; die Filterbeschreibung und die frei formulierte Frage stehen bei den Anweisungen. Das Sprachmodell wird angewiesen, Anweisungen in den Daten nicht zu befolgen; eine Beeinflussung über Freitexte ist damit erschwert, aber nicht ausgeschlossen.
- *Ersetzung von Namen:* Vor der Übermittlung ersetzt Feedcube die Namen von Personen, die im Mandanten ein Benutzerkonto haben, alle E-Mail-Adressen sowie mit „http://“, „https://“ oder „www.“ beginnende Internetadressen, die einen solchen Namensbestandteil oder ein „@“ enthalten, durch Platzhalter und setzt sie im Ergebnis wieder ein. Die Erkennung arbeitet nach festen Regeln und erfasst

nicht jede Schreibweise: Namen erkennt sie nur als ganze Wörter, einzeln stehende Vor- oder Nachnamen nur mit großem Anfangsbuchstaben und mindestens drei Buchstaben und nicht, wenn sie zugleich gebräuchliche Wörter sind (etwa „Frank“ oder „Mai“); einen solchen Nachnamen erkennt sie nach einer Anrede oder einem Titel wie „Frau“ oder „Dr.“. Namen von Personen ohne Benutzerkonto, Spitznamen, Schreibfehler, gebeugte Formen, Namen in Wortzusammensetzungen oder in durchgehender Großschreibung, mittelbare Bezüge sowie Telefonnummern und andere Angaben in Freitexten können daher im Klartext an die KI-Dienste gelangen.

- *Geschützte Antworten:* Antworten, die nach Buchstabe c geschützt sind, übermittelt Feedcube nicht; in eine je nach Funktion übermittelte Anzahl der Abgaben gehen sie jedoch ein. Solange die Schuttschwellen ausgeschaltet sind, gibt es keine geschützten Antworten; dann können alle Antworten der Auswahl bis zur Höchstzahl der jeweiligen Funktion einfließen.
 - *Weitere Verarbeitung:* Der Auftragnehmer verwendet die Inhalte nicht zum Training von KI-Modellen. Mit dem Betreiber des KI-Gateways ist vereinbart, dass Inhalte dort nicht über die Bearbeitung der Anfrage hinaus gespeichert werden (Zero-Data-Retention); für den Betreiber des Sprachmodells gelten die in Anlage 3 genannten Bedingungen. Feedcube speichert die Ergebnisse der Auswertungsfunktionen nicht gesondert; sie werden angezeigt oder in den Bericht übernommen, den die auslösende Person erzeugt. Übersetzungen werden Teil des Textes, für den sie angefordert wurden, und mit ihm gespeichert; Seitentitel von Fragebögen speichert Feedcube nach der Übersetzung automatisch. Die frei formulierte Frage überträgt die Weboberfläche als Adressparameter; sie kann daher bis zu deren Löschung in den Zugriffsprotokollen der Webserver enthalten sein (Abschnitt 4).
 - *Übersetzung:* Die Übersetzungsfunktion in den Eingabemasken, etwa für Fragen, Seitentitel von Fragebögen, Begrüßungs-, Dank- und E-Mail-Texte oder Produktnamen, steht Personen mit einer der Berechtigungen „Fragebögen verwalten“, „Texte verwalten“, „Umfragen verwalten“, „Fragen verwalten“, „Produkte verwalten“ oder „Fachbereiche verwalten“ zur Verfügung, solange die KI-Funktionen im Mandanten freigegeben sind. Sie startet ebenfalls nur auf ausdrückliche Auslösung und übermittelt den zu übersetzenden Text unverändert, also ohne Ersetzung von Namen.
 - *Entscheidung des Auftraggebers:* Der Auftraggeber entscheidet, ob und von wem KI-Funktionen genutzt werden, schaltet sie bei Bedarf über die Freigabe im Mandanten ab und trifft die nötigen Vorgaben für seine Benutzerinnen und Benutzer. Eine eigene Berechtigung für die KI-Funktionen bietet Feedcube nicht. Ist die Freigabe eingeschaltet, kann jede Person die KI-gestützten Auswertungen für die Antworten in ihrem Sichtbereich auslösen, deren Rolle die für die jeweilige Funktion erforderliche Berechtigung enthält: Stimmungs- und Themenanalyse setzen die Berechtigung „Kommentare analysieren“ voraus, die übrigen KI-Auswertungen eine Auswertungs- oder Verwaltungsberechtigung von Feedcube, die Übersetzung eine der oben genannten Verwaltungsberechtigungen. Konten ohne eine dieser Berechtigungen, etwa mit der Standardrolle „Teilnehmer“, können keine KI-Funktion auslösen.
- f) **Freitexte und Einzelanzeigen.** Freitextantworten sind für Personen, deren Sichtbereich sie umfasst, im Wortlaut sichtbar, soweit sie nicht nach Buchstabe c geschützt sind. In Kommentarlisen, Zeitleisten und Einzelansichten können zu einer nicht geschützten Antwort Datum und Uhrzeit der Abgabe und bei Antworten mit Organisationsmerkmalen das Team angezeigt werden; die Ergebnislisten der Stimmungs- und Themenanalyse zeigen zu einem Kommentar das Datum der Abgabe und gegebenenfalls die bewertete Person. Der Export enthält den Abgabezeitpunkt nicht geschützter Antworten. Der Auftraggeber entscheidet, ob Freitextfragen oder Kommentarfelder zu Fragen eingesetzt werden, und weist die Teilnehmenden darauf hin, keine Angaben zu machen, die Rückschlüsse auf sie selbst oder auf andere Personen zulassen.
- g) **Keine automatisierten Einzelentscheidungen.** Feedcube trifft keine automatisierten Entscheidungen im Sinne des Art. 22 DSGVO. Auswertungen über bewertete Personen und Ergebnisse der KI-gestützten

Auswertung sind Hilfsmittel für den Auftraggeber; KI-Ergebnisse können unvollständig oder unzutreffend sein. Entscheidungen über Personen trifft allein der Auftraggeber. Der Auftragnehmer erstellt keine eigenen Auswertungen über Teilnehmende oder bewertete Personen.

- h) **Information der betroffenen Personen.** Die Information der Teilnehmenden sowie der eingeladenen und der bewerteten Personen nach Art. 13 und 14 DSGVO obliegt dem Auftraggeber (§ 3 Abs. 1 der Vereinbarung). Er kann dafür die frei gestaltbaren Begrüßungs-, Dank- und Einladungstexte nutzen, etwa für einen Hinweis auf seine Datenschutzinformation. Die Standardtexte, mit denen Feedcube neue Umfragen und Einladungen vorbelegt und die der Auftraggeber mit der Berechtigung „Texte verwalten“ anpassen kann, sichern in neu eingerichteten Mandanten keine Anonymität zu; in früher eingerichteten Mandanten können die Begrüßungs- und Danktexte Aussagen zur Anonymität enthalten. Der Auftraggeber prüft die Texte vor dem Einsatz und passt sie an seine Befragung und an die eingestellten Schutzwerten an. Spätere Änderungen der Standardtexte wirken sich auf bereits angelegte Umfragen nicht aus. Nutzt der Auftraggeber CourseMate, enthält dessen automatische Feedback-E-Mail an Teilnehmende den Satz, die Antworten würden anonym ausgewertet; der Auftraggeber prüft, ob das für die jeweilige Befragung zutrifft. Die Teilnehmerseite verweist auf Impressum und Datenschutzerklärung des Auftragnehmers zu dessen eigenen Verarbeitungen; die Information der Betroffenen durch den Auftraggeber ersetzt das nicht. Bei persönlichen Einladungen von Personen mit Benutzerkonto weist der Auftraggeber darauf hin, welche Organisationsmerkmale mit der Antwort gespeichert werden (Buchstabe a); bei Umfragen mit bewerteten Personen berücksichtigt er, dass deren Namen auf der Teilnehmerseite angezeigt werden (Buchstabe b).

7. Dauer und Ort der Verarbeitung

Die Verarbeitung erfolgt für die Laufzeit des Hauptvertrags und danach, bis die Daten nach § 11 der Vereinbarung gelöscht oder zurückgegeben sind. Über die Aufbewahrung der Inhalte – insbesondere Umfragen, Antworten, Einladungen, Benutzerkonten und hochgeladene Dateien – entscheidet der Auftraggeber; während der Laufzeit löscht der Auftragnehmer sie nicht von sich aus (§ 11 Abs. 1 der Vereinbarung). Für technische Daten, Protokolle einschließlich des Versandprotokolls der Einladungen und für Datensicherungen gelten die festen Fristen der Anlage 4.

Der Auftragnehmer betreibt Feedcube einschließlich der Datenbanken, der Dateiablage, der Server-Protokolle und der Datensicherungen in Rechenzentren in Deutschland (Anlage 3). KI-Funktionen werden, soweit sie genutzt werden, über ein KI-Gateway mit Endpunkt in Frankfurt am Main von einem Sprachmodell in der Europäischen Union verarbeitet. Die Orte der Verarbeitung bei den Unterauftragsverarbeitern, Ausnahmen davon sowie etwaige Zugriffe aus Drittländern und deren Grundlage nennt Anlage 3.

Anlage 2 – Technische und organisatorische Maßnahmen

Stand: 11.10.2026

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die der Auftragnehmer nach Art. 32 DSGVO für die Verarbeitung im Auftrag trifft. Sie gelten für Feedcube einschließlich der Teilnehmerseite der Befragungen, der Server-Anwendung (Backend), der Datenbanken und der Hosting-Umgebung.

Feedcube wird auf einer Plattform betrieben, die der Auftragnehmer auch für weitere eigene Produkte nutzt. Die Maßnahmen gelten für Feedcube und für die Bestandteile der Plattform, die Feedcube mit den weiteren Produkten teilt, insbesondere Hosting, Datenbankserver, Anmeldung, Benutzerkonten, Protokollierung und Datensicherung. Maßnahmen für Funktionen der weiteren Produkte regeln die Ergänzungen nach § 1 Abs. 2 der Vereinbarung; für die Weiterentwicklung der Maßnahmen gilt § 5 Abs. 2 der Vereinbarung.

1. Vertraulichkeit

Zutrittskontrolle. Der Auftragnehmer betreibt keine eigenen Serverräume. Server, Datenbanken und Datensicherungen befinden sich in Rechenzentren der Hetzner Online GmbH in Deutschland (Anlage 3). Den physischen Schutz stellt der Rechenzentrumsbetreiber sicher, der nach ISO/IEC 27001 zertifiziert ist. Zu den von ihm vertraglich zugesicherten Maßnahmen gehören unter anderem ein elektronisches Zutrittskontrollsystem mit Protokollierung, eine dokumentierte Ausgabe von Zutrittsmedien, eine flächendeckende Videoüberwachung und ein Sicherheitszaun um das Rechenzentrumsgelände.

Zugangskontrolle zur Anwendung.

- Die Weboberfläche lässt sich nur nach Anmeldung mit einem Benutzerkonto nutzen. Teilnehmende einer Befragung benötigen kein Benutzerkonto; sie öffnen die Teilnehmerseite der jeweiligen Umfrage über deren Link oder QR-Code.
- Passwörter müssen mindestens 8 Zeichen lang sein und Groß- und Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten; die Server-Anwendung prüft diese Regel bei jedem Setzen eines Passworts. Wer das eigene Passwort im Profil ändert, muss das bisherige Passwort angeben; dabei beendet die Server-Anwendung alle anderen Anmeldesitzungen des Kontos. Personen mit der Berechtigung „Benutzer verwalten“ können Passwörter in der Benutzerverwaltung ohne Angabe des bisherigen Passworts setzen, auch das eigene, Personen ohne Administratorrolle jedoch nicht für Administratorkonten und nicht für Konten, deren Rolle weiter reicht als die eigene; dabei beendet die Server-Anwendung alle Anmeldesitzungen des betroffenen Kontos, beim eigenen Konto alle außer der des verwendeten Browsers. Wird ein Passwort über einen Link zurückgesetzt, enden ebenfalls alle Anmeldesitzungen des Kontos. API-Schlüssel des Kontos bleiben davon unberührt.
- In der Datenbank werden Passwörter und API-Schlüssel nur als Einweg-Hash gespeichert (von API-Schlüsseln zur Wiedererkennung zusätzlich die ersten Zeichen), Codes zum Zurücksetzen und Festlegen von Passwörtern, BestätigungsCodes der Selbstregistrierung und Sitzungs-Token ebenfalls nur gehasht. Codes aus Passwort- und Registrierungslinks können in den Zugriffsprotokollen der Webserver (Anlage 4 Abschnitt 2 Nr. 14) enthalten sein; sie sind höchstens 24 Stunden gültig. Zugangsdaten zu Cloud-Diensten, die der Auftraggeber anbindet, werden verschlüsselt gespeichert.
- Jede Person kann für ihr Konto eine Zwei-Faktor-Anmeldung mit einer Authenticator-App einrichten (zeitbasierte Einmalcodes, dazu Backup-Codes für den Notfall) und Passkeys nach dem WebAuthn-Standard nutzen, als zweiten Faktor oder zur Anmeldung ohne Passwort; eine Anmeldung mit Passkey verlangt keinen weiteren Faktor.

- Ist die Anmeldung mit Microsoft oder Google auf der Plattform eingerichtet, können sich Personen zusätzlich mit einem Microsoft- oder Google-Konto anmelden, dessen E-Mail-Adresse (bei Microsoft der Anmeldename) der ihres Benutzerkontos entspricht; eine für das Benutzerkonto eingerichtete Zwei-Faktor-Anmeldung gilt dabei weiter. Hat der Auftraggeber seinen Identitätsdienst angebunden (Single Sign-on), nimmt die Anwendung bei der Anmeldung über diesen Anbieter für die E-Mail-Domain des Verzeichnisses nur Konten aus diesem Verzeichnis an; dann gelten dessen Sicherheitsrichtlinien, etwa zur Zwei-Faktor-Anmeldung, und die Zwei-Faktor-Abfrage von Feedcube entfällt.
- Der Auftraggeber kann für die E-Mail-Domain seines angebundenen Verzeichnisses die Anmeldung mit Passwort sperren („Nur SSO“). Für Konten dieser Domain ist dann eine Anmeldung mit Passwort oder Passkey nicht mehr möglich. Die Sperre erfasst nicht die Anmeldung mit einem Konto des jeweils anderen Anbieters (Microsoft bzw. Google), dessen E-Mail-Adresse oder Anmeldename mit der des Benutzerkontos übereinstimmt; bestehende Sitzungen und API-Schlüssel bleiben von ihr unberührt.
- Wiederholte Fehlversuche bei der Anmeldung und bei der Abfrage des zweiten Faktors werden begrenzt und führen zu einer zeitweisen Sperre weiterer Versuche. Auch Anfragen zum Zurücksetzen von Passwörtern und zur Selbstregistrierung sind mengenmäßig begrenzt.
- Die bei der Anmeldung ausgestellten Zugriffstoken gelten 15 Minuten. Erneuert werden sie über ein Sitzungs-Token, das bei jeder Erneuerung ausgetauscht wird. Eine Sitzung verlängert sich mit jeder Erneuerung, die bei Nutzung der Weboberfläche regelmäßig erfolgt, und verfällt spätestens 30 Tage nach der letzten Erneuerung.
- Die Abmeldung beendet auf dem Server die Sitzung des verwendeten Browsers, einschließlich der mit derselben Anmeldung geöffneten Sitzungen in anderen Produkten der Plattform und einer mit ihr geöffneten Ansicht als anderer Benutzer; bereits ausgegebene Zugriffstoken dieser Sitzungen werden sofort ungültig. Ist die Weboberfläche geöffnet, meldet sie nach 60 Minuten ohne Bedienung automatisch ab und beendet die Sitzung dabei wie bei der Abmeldung auch auf dem Server. Wird sie erst nach mehr als 60 Minuten ohne Bedienung wieder geöffnet, beendet sie die Sitzung, statt sie fortzusetzen. Wird der Browser ohne Abmeldung geschlossen, bleibt die Sitzung auf dem Server bis zu ihrem Ablauf bestehen; ist der zentrale Anmelddienst für den Mandanten eingerichtet, kann er die Person bis dahin in diesem Browser ohne erneute Eingabe ihrer Zugangsdaten in einem anderen Produkt der Plattform anmelden. Benutzer sollten sich deshalb, insbesondere an gemeinsam genutzten Geräten, abmelden. Sitzungen auf anderen Geräten oder in anderen Browsern bleiben bestehen, bis sie ablaufen, dort beendet werden, das Passwort des Kontos geändert oder das Konto deaktiviert oder gelöscht wird. Erkennt die Server-Anwendung, dass ein bereits ausgetauschtes Sitzungs-Token erneut verwendet wird, beendet sie die gesamte zugehörige Sitzung.
- Die Cookies für Sitzung und Anmeldung tragen das Attribut „Secure“ und werden daher nur über verschlüsselte Verbindungen übertragen. Über das Sitzungs-Cookie eines Mandanten erneuert, beendet oder übergibt die Server-Anwendung Sitzungen nur auf Anfragen von Seiten dieses Mandanten sowie der zentralen Einstiegsadresse und der zentralen Anmeldung derselben Produktdomain; Anfragen, die eine andere Herkunft angeben, weist sie ab. Der produktübergreifende zentrale Anmelddienst stellt Sitzungen nur bei Seitenaufrufen aus und übergibt sie nur an Seiten des Mandanten der Sitzung und an die zentrale Einstiegsadresse derselben Produktdomain; der Aufruf seiner Abmeldeadresse beendet die Sitzung unabhängig davon, von welcher Seite er ausgeht.
- API-Schlüssel zur Anbindung eigener Systeme des Auftraggebers können nur Personen mit der Berechtigung „API-Schlüssel verwalten“ erzeugen, und zwar für ihr eigenes Konto. Anfragen mit einem API-Schlüssel erhalten die jeweils aktuellen Rechte dieses Kontos. Ein API-Schlüssel gilt bis zu seiner Löschung oder einem beim Erzeugen optional festgelegten Ablaufdatum und wird mit der Deaktivierung oder Löschung des Kontos dauerhaft unwirksam.

Administrative Zugänge.

- Administrative Zugänge zur Hosting-Umgebung, also zu Servern und Containern, Datenbanken, zur Datenbank-Verwaltungsoberfläche und zur Verwaltungsoberfläche der Virtualisierung, sind nicht aus dem öffentlichen Internet erreichbar, sondern nur über ein VPN oder aus privaten Netzsegmenten.
- Zugang erhalten nur die mit dem Betrieb betrauten Personen des Auftragnehmers.

Zugriffskontrolle.

- Der Auftraggeber legt Rollen mit Einzelberechtigungen fest und weist sie den Benutzerkonten zu. Funktionen zur Verwaltung von Benutzern, Rollen, Einstellungen und Inhalten prüfen die erforderliche Berechtigung auf dem Server.
- Rolle, Berechtigungen und Kontostatus werden bei jeder Anfrage an die Schnittstellen von Feedcube aktuell aus der Datenbank gelesen. Änderungen an Rollen und Berechtigungen sowie die Deaktivierung oder Löschung eines Benutzerkontos wirken deshalb ab der nächsten Anfrage; ein deaktiviertes oder gelöscht Konto wird ab dann abgewiesen, auch beim Zugriff über API-Schlüssel.
- Welche Antworten in die Auswertungen einer Person einfließen, richtet sich nach dem Sichtbereich, den ihr der Auftraggeber über Berechtigungen einräumt, etwa Feedback zur eigenen Person, zu eigenen Teams, zu unterstellten Organisationseinheiten oder zu zugeordneten Standorten. Ausgenommen sind insbesondere der abschaltbare Organisations-Benchmark des Dashboards, der Durchschnittswerte über alle Antworten des Mandanten ohne Aufschlüsselung nach Personen oder Organisationseinheiten zeigt, und die weiteren in Anlage 1 Abschnitt 6 d genannten Fälle.
- Personen mit der Administratorrolle können die Anwendung zur Unterstützung anderer Benutzer lesend aus deren Sicht aufrufen („Ansicht als anderer Benutzer“), sofern das betreffende Konto aktiv ist und nicht die Administratorrolle hat. Die Ansicht ist auf 30 Minuten befristet, Änderungen sind in ihr gesperrt, und ihr Beginn wird mit beiden Benutzerkonten protokolliert. Sie endet vorzeitig, wenn das angesehene Konto deaktiviert oder gelöscht wird, wenn die Sitzung des Administrators durch Abmeldung oder Passwortänderung endet oder wenn sein Konto deaktiviert, gelöscht oder aus der Administratorrolle herabgestuft wird.
- Mit den Berechtigungen „Benutzer verwalten“ und „Rollen verwalten“ lassen sich Rollen und Rechte vergeben. Personen ohne Administratorrolle können dabei nur Berechtigungen und Rollen vergeben, die ihre eigene Rolle bereits enthält; die Administratorrolle können sie nicht vergeben, und Konten mit der Administratorrolle oder mit weiterreichenden Berechtigungen können sie weder ändern noch deaktivieren oder löschen. Wer die Berechtigung „Integrationen verwalten“ hat, legt fest, welche Rolle Konten erhalten, die bei angebundenem Identitätsdienst automatisch angelegt werden (Anlage 3 Abschnitt 2 Abs. 1). Der Auftragnehmer empfiehlt, diese Berechtigungen ebenso wie die Administratorrolle nur Personen mit administrativer Aufgabe zu erteilen. Das letzte aktive Administratorkonto eines Mandanten lässt sich weder löschen noch deaktivieren noch herabstufen.
- Personen, die für den Auftragnehmer tätig sind, greifen auf Daten im Mandanten des Auftraggebers nur zu, soweit es für Einrichtung, Betrieb, Wartung und Support oder zur Ausführung einer Weisung erforderlich ist (Need-to-know). Benutzerkonten des Auftragnehmers im Mandanten des Auftraggebers sind in dessen Benutzerverwaltung sichtbar; der Auftraggeber kann sie jederzeit deaktivieren.

Trennungskontrolle.

- Jeder Kunde erhält einen eigenen Mandanten mit eigener Datenbank. Die Mandanten-Datenbanken liegen auf einem gemeinsamen Datenbankserver und werden von derselben Server-Anwendung bedient; die Trennung ist logisch und wird von der Anwendung umgesetzt.
- Jede Anfrage wird einem Mandanten zugeordnet. Zugriffstoken gelten nur für den Mandanten, für den sie ausgestellt wurden, und werden in anderen Mandanten abgewiesen. Persönliche API-Schlüssel sind in der Datenbank des jeweiligen Mandanten hinterlegt und nur dort gültig. Hochgeladene Dateien werden

je Mandant getrennt abgelegt und über Adressen mit einer zufälligen, nicht erratbaren Kennung ausgeliefert; damit etwa Logo und Hintergrundbilder auch auf der Teilnehmerseite erscheinen, setzt der Abruf keine Anmeldung voraus.

- Feedcube teilt sich die Plattform mit weiteren Produkten des Auftragnehmers (derzeit CourseMate, Quipla und Mindsketch). Die Produkte verwenden dieselbe Server-Anwendung, dieselbe Anmeldung und die Datenbank des jeweiligen Mandanten gemeinsam; Benutzerkonten und Rollen eines Mandanten gelten für alle Produkte der Plattform.
- Für die Schnittstelle, über die Umfragen aus vorhandenen Vorlagen automatisiert angelegt werden, kann neben persönlichen API-Schlüsseln ein mandantenübergreifend gültiger Dienstschlüssel eingesetzt werden. Er wird ausschließlich vom Auftragnehmer verwahrt, nur im Kopf der Anfrage angenommen und berechtigt nur zum Anlegen von Umfragen aus Vorlagen; die Antwort enthält den Teilnahmelink samt QR-Code, den Fragebogen der Vorlage, gegebenenfalls die Bezeichnung des angegebenen Produkts sowie Name und interne Kennung einer per E-Mail-Adresse angegebenen bewerteten Person. Jede mit dem Dienstschlüssel angelegte Umfrage und jede Anfrage mit ihm auf eine nicht vorhandene Vorlage wird im Aktivitätsprotokoll des betroffenen Mandanten vermerkt, ohne den Schlüssel selbst. Persönliche API-Schlüssel können Umfragen über diese Schnittstelle nur anlegen, wenn das Konto die Berechtigung „Umfragen verwalten“ hat.
- Neue Mandanten richtet der Auftragnehmer aus einer Vorlage ohne personenbezogene Daten ein. Das erste Administratorkonto erhält kein voreingestelltes Passwort; die berechtigte Person legt es über einen befristeten Link selbst fest.
- Entwicklung und Tests erfolgen nicht mit Daten des Auftraggebers; seine Daten werden nicht in Entwicklungs-, Test- oder Demo-Umgebungen übernommen. Eine Ausnahme, etwa für eine Fehleranalyse, setzt eine Weisung des Auftraggebers voraus; für sie gilt Abschnitt 4.

Pseudonymisierung und Datenminimierung.

- Antworten auf Umfragen werden ohne Benutzerkennung, E-Mail-Adresse und IP-Adresse der antwortenden Person gespeichert (Anlage 1 Abschnitt 6 a).
- Einstellbare Schutzwelken schützen in den Auswertungen Antworten aus zu kleinen Personengruppen und aus Umfragen mit zu wenigen Antworten; sie gelten auch für Berichte, Exporte und KI-Auswertungen. Ihre Wirkung und ihre Grenzen, etwa bei gefilterten Ansichten, beschreibt Anlage 1 Abschnitt 6 c.
- Die KI-Funktionen von Feedcube laufen nicht automatisch, sondern nur auf ausdrückliche Anforderung einer angemeldeten und dazu berechtigten Person im Mandanten des Auftraggebers, nicht über API-Schlüssel, in begrenzter Zahl je Benutzerkonto und nur, solange sie für seinen Mandanten eingeschaltet sind (Anlage 1 Abschnitt 6 e). Bevor Antworten an den KI-Dienst gehen, ersetzt die Anwendung die Namen der im Mandanten angelegten Benutzer sowie E-Mail-Adressen durch Platzhalter; die Zuordnung besteht nur während der jeweiligen Anfrage im Arbeitsspeicher. Namen in Freitexten werden dabei nicht in jedem Fall erkannt, etwa bei Spitznamen, Schreibfehlern oder Personen ohne Benutzerkonto. Kontextangaben beschränkt die Anwendung auf das für die Auswertung Erforderliche, etwa den Monat statt des Zeitpunkts der Abgabe. Der Auftragnehmer verwendet die Inhalte nicht zum Training von KI-Modellen.
- Ein täglicher Löschlauf entfernt technische Daten nach festen Fristen, insbesondere abgelaufene oder widerrufen Sitzungs-Token, Anmeldeversuche, nicht bestätigte Selbstregistrierungen sowie ältere Einträge des Aktivitäts- und des Versandprotokolls (Anlage 4). Inhalte des Auftraggebers löscht der Löschlauf nicht; über ihre Aufbewahrung entscheidet der Auftraggeber.

2. Integrität

Weitergabekontrolle.

- Verbindungen aus dem Internet zur Weboberfläche, zur Teilnehmerseite und zu den Schnittstellen sind mit TLS (HTTPS) verschlüsselt; unverschlüsselte Aufrufe werden auf HTTPS umgeleitet. Die TLS-Verbindung endet am vorgelagerten Webserver der Hosting-Umgebung; zwischen Webserver, Anwendung und Datenbank werden die Daten innerhalb nicht öffentlicher Netzsegmente übertragen.
- Der Auftragnehmer übermittelt Daten nur an die in Anlage 3 genannten Unterauftragsverarbeiter und im Übrigen nur auf Weisung des Auftraggebers, etwa beim Versand von Einladungen an die von diesem festgelegten Empfängerinnen und Empfänger.
- Beim Versand von E-Mails sind die Öffnungs- und die Klickverfolgung des Versanddienstes abgeschaltet.
- Weboberfläche und Teilnehmerseite laden Programmbibliotheken und Schriftarten von den Servern des Auftragnehmers. QR-Codes zu Umfragelinks werden ohne Dienste Dritter erzeugt; das Standard-Profilbild liefern ebenfalls die Server des Auftragnehmers aus.
- Die Teilnehmerseite entfernt das Kennzeichen des Teilnahmelinks nach dem Aufruf aus der Adresszeile, hält es nur für den geöffneten Browser-Tab und gibt die Adresse mit dem Kennzeichen nicht als Herkunftsangabe (Referrer) an andere Server weiter.

Eingabekontrolle.

- Ein Aktivitätsprotokoll hält insbesondere fest: Anmeldungen (mit Passwort, Passkey oder Single Sign-on) und fehlgeschlagene Anmeldeversuche mit Passwort; das Anlegen, Ändern, Deaktivieren und Löschen von Benutzerkonten und Rollen durch berechtigte Personen; der Export der Benutzerliste; Änderungen an Umfragen, Fragen und Stammdaten wie Produkten, Standorten und Teams; Änderungen an Darstellungs- und Datenschutzeinstellungen einschließlich der Freigabe der KI-Funktionen; Löschungen von Umfragen, Antworten, Fragen und Stammdaten, jeweils mit Art und interner Kennung des gelöschten Objekts, aber ohne dessen Inhalt; das Auslösen von KI-Auswertungen, nicht jedoch von KI-Übersetzungen; das Anlegen von Umfragen mit dem Dienstschlüssel und Anfragen mit ihm auf nicht vorhandene Vorlagen. Jeder Eintrag enthält das Ereignis, den Zeitpunkt und die E-Mail-Adresse des handelnden Benutzerkontos, bei Anmelde- und Registrierungsversuchen die eingegebene E-Mail-Adresse und bei Nutzungen des Dienstschlüssels statt einer E-Mail-Adresse einen Hinweis auf den Dienstschlüssel. Verlangt eine Anmeldung mit Passwort oder mit einem Microsoft- oder Google-Konto außerhalb des angebundenen Verzeichnisses einen zweiten Faktor, wird sie erst nach dessen Prüfung als erfolgreich vermerkt. Für Einträge aus der Ansicht als anderer Benutzer gilt Anlage 1 Abschnitt 6 d.
- Der Auftraggeber kann das Aktivitätsprotokoll mit der dafür vorgesehenen Berechtigung einsehen. Die Einträge werden 180 Tage aufbewahrt und danach im täglichen Löschlauf entfernt.
- Zugriffsprotokolle der Webserver und Protokolle der Server-Anwendung dienen der Fehleranalyse und der Abwehr von Angriffen. Sie sind nur den mit dem Betrieb betrauten Personen zugänglich und werden spätestens nach 14 Tagen gelöscht. Im Zugriffsprotokoll der Server-Anwendung sind die Werte von Adressparametern sowie E-Mail-Adressen und tokenartige Bestandteile der aufgerufenen Adressen durch Platzhalter ersetzt. Meldungen, die Feedcube selbst in die Protokolle der Server-Anwendung schreibt, enthalten keine Namen oder E-Mail-Adressen; Benutzerkonten bezeichnen sie, soweit erforderlich, mit ihrer internen Kennung. Fehlerberichte zu unbehandelten Fehlern bereinigt die Server-Anwendung um erkannte E-Mail-Adressen und Token. Die weiteren Produkte der Plattform schreiben in dieselben Protokolle; ihre Meldungen können E-Mail-Adressen und weitere Angaben enthalten und unterliegen denselben Zugriffsbeschränkungen und derselben Löschfrist. Der Auftragnehmer wertet Protokolle nicht aus, um Antworten einzelnen Teilnehmenden zuzuordnen.

- Fragen lassen sich nur mit den Fragetypen von Feedcube speichern. Eingebettete HTML-Inhalte, Skripte und Bildadressen entfernt die Server-Anwendung beim Speichern über die Weboberfläche aus Fragen, Fragebögen sowie Begrüßungs- und Danktexten von Umfragen und Vorlagen. Bei der Ausgabe an Teilnehmende bereinigt sie Fragen und diese Texte in jedem Fall erneut, also auch Inhalte, die auf anderem Weg gespeichert wurden, etwa Standardtexte des Mandanten oder über die Programmierschnittstelle angelegte Umfragen; in den Texten verbleiben nur Formatierungen, Links und eingebettete Bilder oder Bilder aus der Dateiablage der Plattform. Das soll verhindern, dass über Umfrageinhalte Schadcode im Browser von Teilnehmenden ausgeführt wird.

Monitoring der Weboberfläche. Um Fehler und Leistungsprobleme der Weboberfläche zu erkennen, setzt der Auftragnehmer den Dienst Datadog mit Datenspeicherung in der EU ein (Anlage 3). Übermittelt werden technische Nutzungsdaten wie aufgerufene Seiten und Schnittstellenadressen, Bedienschritte, Lade- und Antwortzeiten, Fehlermeldungen, Browser- und Geräteangaben, die IP-Adresse und gegebenenfalls ein daraus abgeleiteter ungefährender Standort. Dabei gilt:

- Auf der Teilnehmerseite und auf den Seiten für Anmeldung, Registrierung, Passwort, Zwei-Faktor-Abfrage, Single Sign-on, Freischaltung und Auswahl der Organisation findet kein Monitoring statt.
- Im Browser werden dafür weder Cookies noch andere Daten gespeichert; die Monitoring-Sitzung besteht nur im Arbeitsspeicher.
- Sitzungen werden nicht aufgezeichnet (keine Sitzungswiedergabe). Bedienschritte werden ohne den Text des angeklickten Elements übermittelt.
- Vor dem Versand werden aus Adressen Abfrageparameter und Fragmente entfernt sowie E-Mail-Adressen und tokenartige Bestandteile ersetzt; in Meldungstext und Stacktrace von Fehlermeldungen werden erkannte E-Mail-Adressen, Token und Zugangsdaten unkenntlich gemacht. Fehlertexte können dennoch Namen oder andere Inhalte enthalten.
- Angemeldete Personen werden nur über ihre interne Benutzerkennung zugeordnet (pseudonym), nicht über Name oder E-Mail-Adresse.
- Die Monitoring-Daten werden spätestens nach 30 Tagen gelöscht.

3. Verfügbarkeit und Belastbarkeit

- Die Rechenzentren verfügen nach den vertraglich zugesicherten Maßnahmen des Betreibers über eine unterbrechungsfreie, redundant ausgelegte Stromversorgung mit Netzersatzanlagen, redundante Kühlung, eine flächendeckende Brandfrüherkennung mit automatischer Alarmierung, eine redundante Netzwerkinfrastruktur und eine ständig aktive Erkennung von DDoS-Angriffen.
- Die Datenbanken werden stündlich gesichert. Die Sicherungen werden rollierend höchstens 3 Tage aufbewahrt und danach automatisch gelöscht.
- Bei Störungen ist die Wiederherstellung aus der jüngsten geeigneten Sicherung das festgelegte Verfahren. Der Auftragnehmer prüft die Wiederherstellbarkeit regelmäßig und anlassbezogen durch Wiederherstellungstests und dokumentiert deren Ergebnisse.
- Anwendung und Datenbank laufen in getrennten Containern; die Datenbank ist nicht aus dem Internet erreichbar. Neue Versionen werden nach einem dokumentierten Verfahren bereitgestellt.

4. Organisatorische Maßnahmen

- Alle Personen, die für den Auftragnehmer tätig sind und Zugang zu personenbezogenen Daten des Auftraggebers erhalten können, sind schriftlich zur Vertraulichkeit und auf das Datengeheimnis nach § 6 DSG verpflichtet. Die Verpflichtung gilt über das Ende ihrer Tätigkeit hinaus.

- Berechtigungen des eigenen Personals werden nach dem Need-to-know-Prinzip vergeben, regelmäßig überprüft und bei Ausscheiden oder Aufgabenwechsel unverzüglich entzogen.
- Daten des Auftraggebers werden nicht auf Arbeitsplatzrechner oder in Entwicklungs- und Testumgebungen kopiert. Ist ein Datenbankauszug ausnahmsweise erforderlich, etwa für eine Migration oder für eine Fehleranalyse auf Weisung des Auftraggebers, wird er zweckgebunden und dokumentiert erstellt, verschlüsselt aufbewahrt und nach Erledigung, spätestens nach 3 Tagen, gelöscht.
- Nicht mehr benötigte Kopien von Daten des Auftraggebers werden so gelöscht, dass sie nicht wiederhergestellt werden können.
- Im Support sieht der Auftragnehmer Daten des Auftraggebers nur ein und übernimmt sie nur in Supportvorgänge, soweit es für die Bearbeitung erforderlich ist.

5. Auftragskontrolle

- Der Auftragnehmer verarbeitet die Daten des Auftraggebers nur nach dessen Weisungen; Einzelweisungen und ihre Umsetzung werden dokumentiert.
- Der Auftragnehmer führt ein Register seiner Unterauftragsverarbeiter. Vor dem Einsatz eines Unterauftragsverarbeiters prüft er dessen Garantien für geeignete technische und organisatorische Maßnahmen und schließt mit ihm eine Vereinbarung nach Art. 28 Abs. 4 DSGVO; für Übermittlungen in Drittländer stützt er sich auf Garantien nach Kapitel V DSGVO.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Der Auftragnehmer dokumentiert seine Verarbeitungstätigkeiten als Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO), diese Maßnahmen, die Aufbewahrungs- und Löschfristen und eine Bewertung der Risiken; geplante Verbesserungen hält er in einem Maßnahmenplan fest.
- Die Maßnahmen werden mindestens jährlich sowie anlassbezogen überprüft und fortgeschrieben, insbesondere nach Sicherheitsvorfällen, vor der Einführung wesentlicher neuer Funktionen und beim Wechsel von Unterauftragsverarbeitern. Dabei wird auch geprüft, ob diese Beschreibung dem tatsächlichen Stand der Anwendung entspricht.
- Für Datenschutzvorfälle besteht ein dokumentierter Prozess mit festgelegten Zuständigkeiten, Einstufung, Eskalation und Meldewegen. Der Auftraggeber wird innerhalb der in der Vereinbarung festgelegten Frist informiert.
- Für Anfragen betroffener Personen besteht ein dokumentierter Prozess. Anfragen, die Daten des Auftraggebers betreffen, leitet der Auftragnehmer an diesen weiter.
- Für die Prüfung der Datenschutzdokumentation und die Bewertung von Vorfällen zieht der Auftragnehmer externe datenschutzrechtliche Beratung hinzu, die zur Verschwiegenheit verpflichtet ist.
- Sicherheitsrelevante Aktualisierungen für Betriebssysteme, Laufzeitumgebungen und eingesetzte Programmbibliotheken werden regelmäßig eingespielt.
- Datenschutz durch Technikgestaltung (Art. 25 DSGVO): Neue Funktionen werden während der Entwicklung auf ihre Auswirkungen auf den Datenschutz geprüft. Beispiele für die datenschutzfreundliche Gestaltung sind die Speicherung von Antworten ohne Personenkennung, die Schuttschwellen der Auswertung und KI-Funktionen, die nur auf Anforderung laufen und in neu eingerichteten Mandanten erst nach Freigabe durch den Auftraggeber zur Verfügung stehen.

Anlage 3 – Unterauftragsverarbeiter

Stand: 11.10.2026

1. Genehmigte Unterauftragsverarbeiter

Die folgenden Unterauftragsverarbeiter sind nach § 6 der Vereinbarung genehmigt. Für Änderungen dieser Liste gilt ebenfalls § 6.

Unterauftragsverarbeiter	Leistung	Betroffene Daten	Ort der Verarbeitung	Grundlage für Drittlandbezug
Hetzner Online GmbH , Gunzenhausen, Deutschland	Hosting der Plattform: Server, Datenbanken, Dateiablage und Datensicherungen	alle in Anlage 1 beschriebenen Daten, einschließlich der Server- und Anwendungsprotokolle und der Datensicherungen	Deutschland	kein Drittlandbezug
Mailgun Technologies, Inc. , San Antonio, Texas, USA (Sinch-Gruppe)	Versand der E-Mails aus Feedcube, z. B. Einladungen zu Befragungen, einmalig oder nach Zeitplan, Registrierungs- und Passwort-E-Mails sowie Hinweise an Administratoren; ohne Öffnungs- und Klickverfolgung	E-Mail-Adresse und gegebenenfalls Name der Empfängerinnen und Empfänger, Betreff und Inhalt der Nachricht samt enthaltenen Links (z. B. persönlicher Teilnahmelink, Bestätigungs- oder Rücksetzlink), Versand- und Zustellprotokolle; Antworten aus Befragungen werden nicht per E-Mail versendet	EU (Deutschland); Zugriffe aus den USA sind nicht ausgeschlossen	EU-US-Datenschutzrahmen (Art. 45 DSGVO, Durchführungsbeschluss (EU) 2023/1795), unter dem Mailgun Technologies, Inc. zertifiziert ist; zusätzlich Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO)
Datadog, Inc. , New York, USA	Fehler- und Leistungsmonitoring der Weboberfläche von Feedcube, ohne Sitzungsaufzeichnung und ohne Speicherung von Cookies oder anderen Daten im Browser; nicht überwacht werden die Teilnehmerseite von Befragungen sowie die Seiten für Anmeldung, Registrierung, Passwort, Zwei-Faktor-Abfrage, Single Sign-on, Freischaltung und Auswahl der Organisation	technische Nutzungsdaten der Personen, die überwachte Seiten aufrufen: IP-Adresse und gegebenenfalls ein daraus abgeleiteter ungefährender Standort, Browser- und Geräteangaben, aufgerufene Seiten- und Schnittstellenadressen ohne Abfrageparameter, Bedienschritte ohne den Text der angeklickten Elemente, Lade- und Antwortzeiten sowie Fehlermeldungen der Weboberfläche; vor dem Versand werden erkannte E-Mail-Adressen, Token und Zugangsdaten in Adressen sowie in Meldungstext und Stacktrace von Fehlermeldungen unkenntlich gemacht, Fehlermeldungen können dennoch Namen oder andere Inhalte enthalten; als Bezug zur Person nur die interne Benutzerkennung, weder Name noch E-Mail-Adresse	EU (Deutschland); Zugriffe aus den USA sind nicht ausgeschlossen	Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) nach der Auftragsverarbeitungsvereinbarung von Datadog; zusätzlich EU-US-Datenschutzrahmen (Art. 45 DSGVO, Durchführungsbeschluss (EU) 2023/1795), unter dem Datadog, Inc. zertifiziert ist

Unterauftragsverarbeiter	Leistung	Betroffene Daten	Ort der Verarbeitung	Grundlage für Drittlandbezug
REQUESTY LTD , London, Vereinigtes Königreich	KI-Gateway: leitet Anfragen der KI-Funktionen an das Sprachmodell weiter und gibt die Ergebnisse zurück; nur bei Nutzung der KI-Funktionen; mit Zero-Data-Retention, d. h. die Inhalte werden nur für die Dauer der Anfrage verarbeitet und nicht gespeichert; keine Verwendung der Inhalte zum Training von Modellen	Inhalte der jeweiligen KI-Anfrage: bei Auswertungen die ausgewählten Freitextantworten sowie Kennzahlen und Verteilungen der Bewertungen mit zugehörigen Angaben wie Frage, Produkt, Standort oder Zeitangaben (Monat der Abgabe, gewählter Zeitraum) sowie gegebenenfalls eine frei formulierte Frage der auswertenden Person, wobei Namen von Personen mit Benutzerkonto und E-Mail-Adressen vorher durch Platzhalter ersetzt werden, soweit Feedcube sie erkennt, sonstige Angaben in Freitexten wie Namen von Personen ohne Benutzerkonto jedoch nicht; bei der Übersetzung der zu übersetzende Text unverändert	Frankfurt am Main, Deutschland (EU-Endpunkt); Zugriffe aus dem Vereinigten Königreich sind nicht ausgeschlossen	Angemessenheitsbeschluss für das Vereinigte Königreich (Art. 45 DSGVO, Durchführungsbeschluss (EU) 2021/1772 in der Fassung des Durchführungsbeschlusses (EU) 2025/2574); ersatzweise Standardvertragsklauseln nach der Auftragsverarbeitungsvereinbarung von Requesty
Mistral AI SAS , Paris, Frankreich (über Requesty eingebunden)	Betrieb des Sprachmodells, das die über Requesty weitergeleiteten KI-Anfragen bearbeitet; nur bei Nutzung der KI-Funktionen; keine Verwendung der Inhalte zum Training von Modellen	wie bei REQUESTY LTD	EU; vorübergehende Übermittlungen an Unterauftragsverarbeiter von Mistral AI außerhalb der EU sind nicht ausgeschlossen	innerhalb der EU kein Drittlandbezug; für etwaige Übermittlungen an Unterauftragsverarbeiter außerhalb des EWR Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) nach den Datenverarbeitungsbedingungen von Mistral AI
Google Cloud EMEA Limited , Dublin, Irland (Cloud Storage for Firebase)	Speicherung und Auslieferung von Dateien, die vor der Umstellung von Feedcube auf die eigene Dateiablage hochgeladen wurden (Altbestand); neue Dateien werden dort nicht abgelegt	Dateien des Altbestands, z. B. Firmenlogo, Hintergrundbilder von Umfragen und Profilbilder; beim Abruf dieser Dateien die technisch übermittelten Verbindungsdaten wie IP-Adresse und Browserangaben, und zwar von Personen mit Benutzerkonto und, wenn eine Teilnehmerseite eine Datei aus dem Altbestand anzeigt, etwa Logo oder Hintergrundbild, auch von Teilnehmenden; keine Antworten aus Befragungen	Rechenzentren von Google; eine Verarbeitung außerhalb des EWR, insbesondere in den USA, ist nicht ausgeschlossen	Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) nach dem Cloud Data Processing Addendum von Google; für Google LLC (USA) zusätzlich EU-US-Datenschutzrahmen (Art. 45 DSGVO, Durchführungsbeschluss (EU) 2023/1795), unter dem Google LLC zertifiziert ist

Unterauftragsverarbeiter	Leistung	Betroffene Daten	Ort der Verarbeitung	Grundlage für Drittlandbezug
Atlassian Pty Ltd , Sydney, Australien (Jira Service Management)	Ticketsystem des Auftragnehmers für Support- und Bestellanfragen sowie für sonstige Anfragen des Auftraggebers und betroffener Personen	Inhalte der Anfragen samt Anhängen, Name und Kontaktdaten der anfragenden Personen, technische Fehlerangaben, Bearbeitungsvermerke; Daten aus Feedcube nur, soweit sie in einer Anfrage enthalten sind oder bei ihrer Bearbeitung beigefügt werden (z. B. Auskunfts- oder Löschnachweise)	Rechenzentren von Atlassian und ihren Dienstleistern; eine Verarbeitung außerhalb des EWR, insbesondere in Australien und den USA, ist nicht ausgeschlossen	Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) nach der Auftragsverarbeitungsvereinbarung von Atlassian, da für Australien kein Angemessenheitsbeschluss besteht; für Atlassian, Inc. und weitere US-Gesellschaften der Atlassian-Gruppe zusätzlich EU-US-Datenschutzrahmen (Art. 45 DSGVO, Durchführungsbeschluss (EU) 2023/1795)
Microsoft Ireland Operations Limited , Dublin, Irland (Microsoft 365, Exchange Online)	E-Mail-Postfächer des Auftragnehmers, z. B. office@feedcube.net und support@feedcube.net, für die Kommunikation mit dem Auftraggeber, insbesondere Weisungen, Meldungen von Verletzungen des Schutzes personenbezogener Daten sowie Support- und sonstige Anfragen	Inhalte von E-Mails samt Anhängen, Namen und E-Mail-Adressen von Absendern und Empfängern; Daten aus Feedcube nur, soweit sie in Nachrichten enthalten sind	EU; Zugriffe aus Drittländern, insbesondere den USA, sind nicht ausgeschlossen	Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) nach dem Datenschutznachtrag zu den Produkten und Services von Microsoft

- (1) Für jeden Unterauftragsverarbeiter gilt eine Vereinbarung nach Art. 28 Abs. 4 DSGVO, die ihm Datenschutzpflichten auferlegt, die denen dieser Vereinbarung im Wesentlichen entsprechen. Mistral AI ist nicht unmittelbar vom Auftragnehmer beauftragt, sondern über Requesty eingebunden; maßgeblich sind die Vereinbarung zwischen Requesty und Mistral AI und die Datenverarbeitungsbedingungen von Mistral AI.
- (2) Die Spalte „Grundlage für Drittlandbezug“ nennt, worauf eine Übermittlung in ein Drittland oder ein Zugriff aus einem Drittland gestützt ist: auf einen Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DSGVO oder auf geeignete Garantien nach Art. 46 DSGVO, insbesondere die Standardvertragsklauseln nach dem Durchführungsbeschluss (EU) 2021/914. Sind neben einem Angemessenheitsbeschluss Standardvertragsklauseln vereinbart, stützt sich die Übermittlung auf diese, wenn der Beschluss wegfällt; der Auftragnehmer passt diese Anlage dann an.
- (3) Requesty und Mistral AI erhalten Daten nur, wenn KI-Funktionen genutzt werden. Google ist nur beteiligt, soweit für den Auftraggeber noch Dateien aus dem Altbestand gespeichert sind. Atlassian und Microsoft verarbeiten Daten aus Feedcube nur, soweit sie in Anfragen oder Nachrichten enthalten sind.

- (4) Die genannten Anbieter setzen ihrerseits Unterauftragsverarbeiter ein, etwa Betreiber von Rechenzentren und Cloud-Diensten oder Gesellschaften ihrer Unternehmensgruppe für Betrieb und Support. Sie führen diese in eigenen veröffentlichten Listen und haben sich verpflichtet, ihnen gleichwertige Datenschutzpflichten aufzuerlegen und Übermittlungen in Drittländer nach Kapitel V DSGVO abzusichern. So betreibt Requesty das KI-Gateway in Rechenzentren der Amazon Web Services, Inc. in Frankfurt am Main; für etwaige Zugriffe dieses Anbieters aus den USA hat Requesty eine Transfer-Folgenabschätzung mit ergänzenden Maßnahmen erstellt. Der Auftragnehmer stellt dem Auftraggeber die jeweils aktuellen Listen auf Anfrage zur Verfügung.
- (5) Nach den Bedingungen des KI-Gateways dürfen keine Daten von Kindern, keine staatlichen Identifikationsnummern und keine Zahlungskartendaten übermittelt werden. Für den Einsatz der KI-Funktionen gilt deshalb § 3 Abs. 2 lit. f der Vereinbarung.

2. Anmeldung über Identitätsdienste

- (1) Bindet der Auftraggeber seinen eigenen Identitätsdienst an (Microsoft Entra ID oder Google Workspace), authentifiziert dieser Dienst die Personen des Auftraggebers auf Grundlage des Vertrags zwischen dem Auftraggeber und dem jeweiligen Anbieter. Der Anbieter ist insoweit für den Auftraggeber tätig und kein Unterauftragsverarbeiter des Auftragnehmers. Meldet sich eine Person über diesen Anbieter mit einer E-Mail-Adresse der angebundenen Domain an, nimmt Feedcube die Anmeldung nur aus dem Verzeichnis des Auftraggebers an. Hat die Person noch kein Benutzerkonto, legt Feedcube bei dieser ersten Anmeldung automatisch eines an, mit dem Namen aus dem Verzeichnis, als E-Mail-Adresse bei Microsoft dem Anmeldenamen und bei Google der bestätigten E-Mail-Adresse des Kontos, und mit der Rolle, die der Auftraggeber bei der Anbindung gewählt hat; ohne gültige Rolle entsteht ein noch nicht freigeschaltetes Konto ohne Berechtigungen. Feedcube erhält vom Anbieter die für die Anmeldung erforderlichen Angaben, insbesondere E-Mail-Adresse, Name und Kennungen von Konto und Verzeichnis. Für die Anbindung speichert Feedcube die Kennung des Verzeichnisses und die Domain, Kennung, Name und E-Mail-Adresse des Kontos, mit dem die Anbindung eingerichtet wurde, das Benutzerkonto, das sie in Feedcube eingerichtet hat, die Rolle für automatisch angelegte Konten, die Einstellung „Nur SSO“ und die vom Anbieter ausgestellten Zugangsdaten in verschlüsselter Form.
- (2) Personen mit einem bestehenden Benutzerkonto können sich außerdem mit einem eigenen Microsoft- oder Google-Konto anmelden, dessen E-Mail-Adresse (bei Microsoft der Anmeldenamen) mit der ihres Benutzerkontos übereinstimmt; das ist auch ohne Anbindung eines Identitätsdienstes durch den Auftraggeber möglich. Ein neues Benutzerkonto entsteht auf diesem Weg nicht. Die Authentifizierung übernimmt der jeweilige Anbieter nach den Bedingungen, die für das Konto der Person gelten; der Auftragnehmer setzt den Anbieter dabei nicht zur Verarbeitung von Daten des Auftraggebers in seinem Auftrag ein. Die Anmeldung läuft über Anwendungsregistrierungen des Auftragnehmers bei Microsoft und Google. Der Anbieter erhält die für den Anmeldevorgang nötigen Angaben, etwa die Rücksprungadresse, einen signierten, aber lesbaren Anmeldestatus mit der Adresse der Organisation in Feedcube und, wenn die Person ihre E-Mail-Adresse bereits eingegeben hat, diese als Anmeldehinweis. Feedcube erhält vom Anbieter insbesondere E-Mail-Adresse, Name und eine Kennung des Kontos.

3. Selbst betriebene Komponenten und gemeinsame Plattform

- (1) Anwendung, Schnittstellen, Datenbanken, Dateiablage, Server- und Anwendungsprotokolle sowie Datensicherungen betreibt der Auftragnehmer selbst auf der Infrastruktur von Hetzner nach Abschnitt 1. Dazu gehört auch der zentrale Anmeldedienst unter id.eduenio.net, über den die Anmeldung in den

Produkten der Plattform zusammengeführt werden kann. Ist er für den Mandanten des Auftraggebers eingerichtet, speichert er dafür ein Cookie für die Anmeldesitzung im Browser. Die Weboberfläche prüft seine Erreichbarkeit; dabei gelangen die IP-Adresse und die Adresse des Mandanten in die Server-Protokolle des Anmeldedienstes (Anlage 4 Abschnitt 2 Nr. 14).

- (2) Feedcube läuft auf einer Plattform, die der Auftragnehmer auch für seine weiteren Produkte CourseMate, Quipla und Mindsketch nutzt. Server-Anwendung, Schnittstellen und die Datenbank des Auftraggebers sind für diese Produkte gemeinsam, ebenso die Benutzerkonten und die Anmeldung.
- (3) Die weiteren Produkte und die Dienste, die nur sie nutzen, sind nicht Gegenstand dieser Vereinbarung, etwa die Dokumentbearbeitung mit Collabora Online, Videokonferenzen mit Jitsi Meet und die Anbindung von Cloud-Dokumenten oder Online-Meetings bei Microsoft oder Google. Die Funktionen von Feedcube übermitteln keine Daten an diese Dienste. Die gemeinsame Einstellungsmaske „Integrationen“ ist auch aus Feedcube erreichbar; verknüpft der Auftraggeber dort ein Microsoft- oder Google-Konto für Cloud-Dokumente oder Online-Meetings, dient das ausschließlich den weiteren Produkten, wobei Kontodaten beim Anbieter abgerufen und dort ein Ordner mit der Kennung der Organisation angelegt werden kann. Bucht der Auftraggeber eines der weiteren Produkte, gelten dafür gesonderte Ergänzungen zu dieser Vereinbarung; für nicht gebuchte Produkte gilt § 1 Abs. 2 der Vereinbarung.
- (4) Neue Bilder lässt Feedcube nur aus der eigenen Dateiablage einbinden. Sind aus früheren Versionen noch Adressen fremder Server gespeichert, etwa für Logo, Hintergrund- oder Profilbilder, laden die Browser der Personen, die diese Inhalte anzeigen, sie von dort. Den Betreiber dieses Servers setzt nicht der Auftragnehmer ein; er ist kein Unterauftragsverarbeiter.

Anlage 4 – Aufbewahrungs- und Löschfristen

Stand: 11.10.2026

1. Grundsätze

- (1) Diese Anlage legt fest, wie lange der Auftragnehmer die Daten aufbewahrt, die er im Auftrag des Auftraggebers in Feedcube verarbeitet, und wie sie gelöscht werden. Feedcube läuft auf einer gemeinsamen Plattform mit den weiteren Produkten des Auftragnehmers (CourseMate, Quipla, Mindsketch); die Benutzerkonten des Auftraggebers gelten für alle Produkte dieser Plattform. Für Daten in weiteren Produkten, die der Auftraggeber bucht, gelten die gesonderten Ergänzungen nach § 1 Abs. 2 der Vereinbarung.
- (2) Über die Aufbewahrung der Inhalte entscheidet der Auftraggeber. Inhalte sind insbesondere Benutzerkonten, Organisations- und Stammdaten, Umfragen, Einladungen, Antworten und hochgeladene Dateien. Sie bleiben gespeichert, bis sie in der Anwendung gelöscht werden oder der Auftraggeber ihre Löschung nach § 2 der Vereinbarung anweist, längstens bis zu ihrer Löschung nach Ende des Hauptvertrags (Abschnitt 3). Der Auftragnehmer löscht Inhalte während der Vertragslaufzeit nicht von sich aus.
- (3) Für technische Daten und Protokolle, darunter das Versandprotokoll der Einladungen, gelten die festen Fristen nach Abschnitt 2. In den Datenbanken setzt sie ein automatischer Löschlauf um, der täglich für alle Mandanten der Plattform läuft und je Lauf die Zahl der gelöschten Einträge protokolliert. Bei planmäßigem Betrieb werden Daten damit spätestens einen Tag nach Ablauf ihrer Frist gelöscht, Daten mit einer Frist von 24 Stunden spätestens nach 48 Stunden; die Angaben „spätestens nach 48 Stunden“ in Abschnitt 2 stehen unter diesem Vorbehalt. Entfällt ein Lauf, holt der nächste Lauf die fälligen Löschungen nach. Inhalte nach Absatz 2 löscht der Löschlauf nicht. Protokolle auf den Servern werden durch automatische Rotation gelöscht, Daten bei Unterauftragsverarbeitern von diesen nach den Fristen in Abschnitt 2.
- (4) Löschungen in der Anwendung wirken sofort und lassen sich dort nicht rückgängig machen. Aus den Datensicherungen scheiden gelöschte Daten nach Abschnitt 2 Nr. 20 aus.
- (5) Löschungen, die der Auftraggeber anweist, führt der Auftragnehmer unverzüglich aus und dokumentiert sie. Auf Anforderung bestätigt er sie schriftlich oder in elektronischer Form (z. B. E-Mail).
- (6) Exporte, Berichte und andere Kopien, die Benutzer des Auftraggebers herunterladen oder außerhalb von Feedcube ablegen, verwaltet der Auftraggeber in eigener Verantwortung.

2. Fristen während der Vertragslaufzeit

In diesem Abschnitt beziehen sich Verweise auf „Nr.“ auf die fortlaufenden Nummern der folgenden Tabellen und Verweise auf „Abs.“ ohne weitere Angabe auf die Absätze im Anschluss an die Tabellen.

Inhalte des Auftraggebers

Nr.	Daten	Aufbewahrung und Löschung
1	Benutzerkonten: Name, E-Mail-Adresse, Rolle, Anmeldedaten (Passwort-Hash, zweiter Faktor, Passkeys), Profilbild sowie Zuordnungen zu Standorten, Teams, Fachbereichen und im Organigramm, auch aus dem Organigramm entfernte Einträge	Bis zur Löschung in der Anwendung oder auf Weisung des Auftraggebers, längstens bis zur Löschung nach Abschnitt 3. In der Anwendung werden Konten in der Benutzerverwaltung mit der Berechtigung „Benutzer verwalten“ gelöscht, Administratorkonten und Konten mit weiterreichenden Berechtigungen nur von Personen mit der Administratorrolle; Personen mit der Rolle „Teilnehmer“ können ihr eigenes Konto unter den Voraussetzungen der Anlage 1 Abschnitt 1 selbst löschen. Deaktivierte und noch nicht freigeschaltete Konten, etwa aus einer bestätigten Selbstregistrierung oder der ersten Anmeldung über einen angebundenen Identitätsdienst (Anlage 3 Abschnitt 2 Abs. 1), bleiben bis zu ihrer Löschung bestehen. Was mit einem Konto gelöscht wird und was bestehen bleibt, beschreibt Abs. 1.
2	Organisations- und Stammdaten: Standorte, Teams, Positionen, Organigramm, Fachbereiche, Bewertungsgegenstände (in Feedcube „Produkte“), Fragen, Fragebögen und Texte	Bis zur Löschung in der Anwendung oder auf Weisung des Auftraggebers, längstens bis zur Löschung nach Abschnitt 3. Das Löschen von Stammdaten kann zugeordnete Umfragen, Antworten oder Zuordnungen mitlöschen (Abs. 2).
3	Umfragen (Fragebogen, Einstellungen, Teilnahmelinks) und Antworten (Bewertungen, Freitexte, Abgabezeitpunkt, Zuordnungsmerkmale wie Bewertungsgegenstand, Standort, Team oder bewertete Person)	Bis zur Löschung in der Anwendung oder auf Weisung des Auftraggebers, längstens bis zur Löschung nach Abschnitt 3. Umfragen werden mit der Berechtigung „Umfragen verwalten“ gelöscht, einzelne Antworten mit der Berechtigung „Feedback löschen“ im Rahmen des Sichtbereichs der löschenden Person. Einzelheiten beschreibt Abs. 2.
4	Einladungsdaten: Empfängerlisten (E-Mail-Adresse, gegebenenfalls Name), persönliche Teilnahmelinks, Zeitpläne für den Versand	Wie die zugehörige Umfrage; sie werden mit ihr gelöscht. Einladungen an Personen mit Benutzerkonto entfallen außerdem mit deren Konto. Für das Versandprotokoll gilt Nr. 8.
5	Hochgeladene Dateien, z. B. Logo, Hintergrundbilder, Bilder in Umfragen und Vorlagen, Profil- und Teambilder, einschließlich des Altbestands früher hochgeladener Dateien bei Google (Anlage 3)	Bis zur Löschung nach Abschnitt 3, sofern der Auftraggeber nicht vorher ihre Löschung anweist. Ersetzt oder entfernt der Auftraggeber eine Datei in der Anwendung oder löscht er den zugehörigen Datensatz, kann die Datei bis dahin in der Dateiablage verbleiben. Auf Weisung löscht der Auftragnehmer einzelne Dateien früher, etwa zur Erfüllung eines Löschantrags.
6	Ergebnisse der KI-Funktionen	Keine gesonderte Speicherung in Feedcube. Die Ergebnisse werden angezeigt. Übernimmt der Auftraggeber sie in Inhalte, etwa als übersetzten Fragetext, gelten deren Fristen; heruntergeladene Berichte verwaltet er selbst (Abschnitt 1 Abs. 6).
7	Exportdateien, die Feedcube für einen Download auf dem Server erzeugt	Nur vorübergehend. Nach dem Download fordert die Weboberfläche die Löschung der Datei an. Nicht abgerufene oder nicht gelöschte Dateien entfernt Feedcube, sobald sie älter als eine Stunde sind, beim nächsten Export oder beim nächsten Abruf einer Exportdatei auf demselben Server; eine abgelaufene Datei wird nicht mehr ausgeliefert. Bis dahin verbleiben sie auf dem Server.

Technische Daten und Protokolle

Nr.	Daten	Aufbewahrung und Löschung
8	Versandprotokoll der Einladungen in Feedcube: Empfängerin oder Empfänger, Betreff, Inhalt (beim Versand nach Zeitplan einschließlich des persönlichen Teilnahmelinks), Versandzeitpunkt und -status	90 Tage nach dem Versand ; Löschung durch den täglichen Löschlauf. Mit einer Umfrage wird auch das Versandprotokoll ihrer Einladungen sofort gelöscht.
9	Sitzungs-Token, auch der zentralen Anmeldung, mit IP-Adresse und Browser-Kennung; Abfragen des zweiten Faktors (mit IP-Adresse) und für Passkeys; Sperrliste widerrufener oder eingelöster Token (nur Token-Kennung, Zeitpunkt und gegebenenfalls Grund)	Sitzungs-Token und Abfragen: bis zum Ablauf oder Widerruf, danach höchstens zwei Tage ; Löschung durch den täglichen Löschlauf. Jedes Sitzungs-Token gilt höchstens 30 Tage ab seiner Ausstellung; bei jeder Erneuerung wird ein neues mit voller Laufzeit ausgestellt und das bisherige widerrufen, sodass eine genutzte Sitzung spätestens 30 Tage nach der letzten Erneuerung verfällt (Anlage 2 Abschnitt 1). Abfragen des zweiten Faktors und für Passkeys gelten 5 Minuten. Sperrliste: bis die längste Laufzeit eines Tokens und ein weiterer Tag verstrichen sind; Einträge, die alle Sitzungen einer Anmeldung sperren, darüber hinaus, solange zu dieser Anmeldung noch Sitzungs-Token gespeichert sind; Löschung durch den täglichen Löschlauf. Zugriffstoken werden nicht gespeichert.
10	Codes aus Links zum Festlegen oder Zurücksetzen des Passworts	24 Stunden (Gültigkeit); danach entfernt der tägliche Löschlauf sie, spätestens nach 48 Stunden.
11	Versuche, die zur Begrenzung von Fehlversuchen gespeichert werden, z. B. bei Anmeldung, Registrierung und zweitem Faktor: IP-Adresse, eingegebene E-Mail-Adresse, Kontokennung oder Kennung der Abfrage des zweiten Faktors, Zeitpunkt, Ergebnis; ferner Zähler zur Begrenzung von Anfragen an die KI-Funktionen (Kontokennung, Zeitpunkt)	24 Stunden ; Löschung durch den täglichen Löschlauf, spätestens nach 48 Stunden. Dieselben Angaben können zusätzlich im Aktivitätsprotokoll (Nr. 13) und in den Server-Protokollen (Nr. 14) enthalten sein; dort gelten deren Fristen.
12	Unbestätigte Selbstregistrierungen: Name, E-Mail-Adresse, Passwort-Hash, Bestätigungscode (als Hash)	Bis zum Ablauf des Bestätigungscode (24 Stunden) ; danach Löschung durch den täglichen Löschlauf, spätestens 48 Stunden nach der letzten Registrierungsanfrage. Mit der Bestätigung entsteht ein Benutzerkonto (Nr. 1).
13	Aktivitätsprotokoll der Anwendung: Zeitpunkt, Ereignis (z. B. Anmeldung, Änderung, Löschung), E-Mail-Adresse des handelnden Benutzerkontos, bei Anmelde- und Registrierungsversuchen gegebenenfalls die eingegebene E-Mail-Adresse, bei der Ansicht als anderer Benutzer zusätzlich die E-Mail-Adresse des angesehenen Kontos; Einträge der weiteren Produkte der Plattform können Namen und E-Mail-Adressen weiterer Personen enthalten	180 Tage ; Löschung durch den täglichen Löschlauf.

Nr.	Daten	Aufbewahrung und Löschung
14	Zugriffsprotokolle der Webserver und Protokolle der Server-Anwendung: IP-Adresse, Zeitpunkt, aufgerufene Adresse, Statuscode, gegebenenfalls Herkunftsadresse, Browser-Kennung und Fehlermeldungen; in den Zugriffsprotokollen der Webserver kann die Adresse ihre Parameter enthalten (z. B. Kennzeichen persönlicher Teilnahmelinks oder E-Mail-Adressen), im Zugriffsprotokoll der Server-Anwendung sind Parameterwerte, E-Mail-Adressen und Token durch Platzhalter ersetzt; Meldungen der weiteren Produkte der Plattform in den Protokollen der Server-Anwendung können E-Mail-Adressen enthalten (Anlage 2 Abschnitt 2)	14 Tage ; automatische Rotation und Löschung auf den Servern. Einzelne Einträge, die zur Aufklärung eines konkreten Sicherheitsvorfalls benötigt werden, bewahrt der Auftragnehmer gesondert und nur bis zum Abschluss der Aufklärung auf; § 9 der Vereinbarung bleibt unberührt. Zur Verwendung der Protokolle siehe Abs. 4.

Daten bei Unterauftragsverarbeitern (Anlage 3)

Nr.	Daten	Aufbewahrung und Löschung
15	Monitoring-Daten der Web-oberfläche beim Dienst für Fehler- und Leistungsüberwachung (Datadog)	30 Tage ; zeitgesteuerte Löschung beim Anbieter.
16	Versand- und Zustellprotokolle sowie gegebenenfalls zwischengespeicherte Nachrichten beim E-Mail-Versanddienst (Mailgun)	Nach den Aufbewahrungsfristen des Versanddienstes, höchstens 30 Tage ; zeitgesteuerte Löschung beim Anbieter.
17	Inhalte von KI-Anfragen und -Ergebnissen beim KI-Gateway (Requesty)	Keine Speicherung über die Bearbeitung der Anfrage hinaus (Zero-Data-Retention).
18	Inhalte von KI-Anfragen und -Ergebnissen beim Betreiber des Sprachmodells (Mistral AI)	Nach den Datenverarbeitungsbedingungen des Modellbetreibers (Anlage 3). Der Auftragnehmer teilt dem Auftraggeber die jeweils geltende Frist auf Anfrage mit.

Supportanfragen und Datensicherungen

Nr.	Daten	Aufbewahrung und Löschung
19	Personenbezogene Daten aus Feedcube in Supportanfragen: Daten, die der Auftraggeber einer Anfrage beifügt oder die bei ihrer Bearbeitung in das Ticketsystem oder die E-Mail-Postfächer des Auftragnehmers übernommen werden (Anlage 3), z. B. Antworten, Bildschirmfotos oder Exportdateien	Bis sie für die Bearbeitung der Anfrage nicht mehr erforderlich sind, höchstens 24 Monate nach Abschluss der Anfrage und längstens bis zur Löschung nach Abschnitt 3; danach Löschung oder Anonymisierung. Kontaktdaten der anfragenden Personen und die Kommunikation zur Anfrage verarbeitet der Auftragnehmer als Verantwortlicher (§ 1 Abs. 3 der Vereinbarung); sie unterliegen nicht dieser Anlage.
20	Datensicherungen der Datenbanken und, soweit gesichert, der Dateiablage	Höchstens 3 Tage. Die Datenbanken werden stündlich gesichert, ältere Sicherungen rollierend gelöscht. Gelöschte Daten sind damit spätestens 3 Tage nach ihrer Löschung in keiner Sicherung mehr enthalten. Sicherungen dienen ausschließlich der Wiederherstellung (Abs. 3).

(1) **Löschen eines Benutzerkontos.** Mit einem Benutzerkonto werden sofort gelöscht:

- die Kontodaten der Person mit Passwort-Hash, Merkmalen des zweiten Faktors (zu Passkeys siehe unten), Sitzungs-Token und API-Schlüsseln,
- ihre Zuordnungen zu Standorten und Teams sowie ihr Eintrag im Organigramm,
- Einladungen, die an die Person als Benutzer gerichtet sind,
- alle Antworten, in denen die Person bewertet wurde.

Darüber hinaus gilt:

- Umfragen, die die Person angelegt hat, bleiben samt ihren Einladungen erhalten; die Angabe der anlegenden Person entfällt. Antworten auf diese Umfragen bleiben erhalten, soweit die Person darin nicht selbst bewertet wurde; der Auftraggeber kann sie mit der Berechtigung „Feedback löschen“ im Rahmen des Sichtbereichs der löschenden Person löschen.
- Umfragen, in denen die Person bewertet wird, bleiben erhalten; Name und Benutzerkennung der Person bleiben in der Seitenzuordnung dieser Umfragen gespeichert und können auf der Teilnehmerseite weiter angezeigt werden, bis der Auftraggeber die Zuordnung ändert oder die Umfrage löscht. Der Auftraggeber prüft solche Umfragen deshalb nach der Löschung.
- Passkeys und Fachbereichszuordnungen der Person entfernt der tägliche Löschlauf.
- Einträge im Versandprotokoll (Nr. 8), im Aktivitätsprotokoll (Nr. 13) und in den Server-Protokollen (Nr. 14) werden nach deren Fristen gelöscht, das Profilbild nach Nr. 5.
- Hatte die Person im Organigramm unterstellte Personen, rücken diese mit ihren eigenen Unterstellten eine Ebene nach oben, also unter die übergeordnete Person der gelöschten Person oder auf die oberste Ebene. Das wirkt sich auf die Organisationsmerkmale künftiger Antworten und auf die Sichtbereiche nach Anlage 1 Abschnitt 6 d aus; der Auftraggeber prüft das Organigramm deshalb nach der Löschung und ordnet unterstellte Personen bei Bedarf neu zu.
- Das letzte aktive Administratorkonto des Mandanten lässt sich nicht löschen.
- Weil die Benutzerkonten für alle Produkte der Plattform gelten, endet mit der Löschung auch der Zugang der Person zu den weiteren Produkten des Auftragnehmers. Für ihre Daten in diesen Produkten gelten die gesonderten Ergänzungen; auf Weisung löscht der Auftragnehmer auch diese Daten.
- Sollen die Bewertungen einer ausscheidenden Person erhalten bleiben, deaktiviert der Auftraggeber ihr Konto, statt es zu löschen.

- (2) **Löschen von Umfragen, Antworten und Stammdaten.** Mit einer Umfrage werden in einem Vorgang ihre Antworten, ihre Einladungen und Zeitpläne samt Empfängerlisten und persönlichen Teilnahmelinks sowie das Versandprotokoll ihrer Einladungen gelöscht. Im Übrigen gilt:
- Einzelne Antworten löscht der Auftraggeber mit der Berechtigung „Feedback löschen“ im Rahmen des Sichtbereichs der löschenden Person. Bewertet eine Abgabe mehrere Personen, speichert Feedcube je bewertete Person eine eigene Antwort, die einzeln gelöscht wird.
 - Erscheinen Antworten zu Umfragen, die mit einer früheren Version von Feedcube gelöscht wurden, noch in den Auswertungen, kann der Auftraggeber sie auf diesem Weg löschen oder ihre Löschung beim Auftragnehmer anweisen.
 - Das Löschen eines Bewertungsgegenstands (in Feedcube „Produkt“, z. B. ein Kurs oder eine Leistung) löscht die zugehörigen Umfragen samt Antworten, Einladungen und Versandprotokoll sowie alle übrigen Antworten zu diesem Bewertungsgegenstand.
 - Das Löschen einer Frage löscht die Werte und Freitexte aller Antworten zu dieser Frage; die übrigen Angaben dieser Antworten bleiben erhalten.
 - Beim Löschen eines Standorts bleiben die zugeordneten Umfragen und Antworten erhalten und werden „Keine Standortangabe“ zugeordnet; die Zuordnung von Benutzerkonten zum Standort entfällt.
 - Das Löschen weiterer Stammdaten wie Teams, Positionen oder Fachbereiche kann Zuordnungen in Umfragen, Antworten und Benutzerkonten entfernen und untergeordnete Stammdaten mitlöschen.
 - Wird eine Person aus dem Organigramm entfernt, rücken ihre direkt unterstellten Personen mit ihren eigenen Unterstellten eine Ebene nach oben; Benutzerkonto und Antworten bleiben erhalten. Der Organigramm-Eintrag wird dabei nur deaktiviert und bleibt mit seinen Angaben (Team, Position, frühere übergeordnete Person) gespeichert, bis das Benutzerkonto gelöscht wird; auf Weisung löscht der Auftragnehmer ihn früher.
- (3) **Wiederherstellung aus einer Datensicherung.** Muss der Auftragnehmer Daten des Auftraggebers aus einer Datensicherung wiederherstellen, entspricht der wiederhergestellte Bestand dem Zeitpunkt der Sicherung; diesen Zeitpunkt teilt er dem Auftraggeber mit. Löschungen, die der Auftraggeber danach angewiesen hat, führt der Auftragnehmer erneut aus. Löschungen, die danach in der Anwendung vorgenommen wurden, führt er erneut aus, soweit sie sich aus seinen Protokollen ergeben oder der Auftraggeber sie benennt; der Auftraggeber kann sie auch selbst in der Anwendung wiederholen. Fristgebundene Löschungen holt der tägliche Löschlauf bei seinem nächsten Lauf nach.
- (4) **Verwendung der Protokolle.** Der Auftragnehmer verwendet die Daten nach Nr. 11, 13 und 14 nur für den Betrieb, die Fehleranalyse und die Sicherheit von Feedcube sowie zur Ausführung von Weisungen des Auftraggebers. Er wertet sie nicht aus, um Antworten einzelnen Teilnehmenden zuzuordnen.

3. Vertragsende

- (1) Nach Ende des Hauptvertrags löscht der Auftragnehmer die Daten des Auftraggebers in Feedcube innerhalb der Frist nach § 11 Abs. 4 der Vereinbarung, also spätestens 30 Tage nach Vertragsende und vorher nur auf Weisung des Auftraggebers; ist eine fristgerecht verlangte Rückgabe dann noch nicht abgeschlossen, löscht er unverzüglich nach ihrem Abschluss. Gelöscht werden insbesondere:
- die Datenbank des Mandanten mit allen Benutzerkonten, Organisations- und Stammdaten, Umfragen, Einladungen, Antworten und den darin geführten Protokollen,
 - die Dateien des Auftraggebers in der Dateiablage einschließlich des Altbestands bei Google (Anlage 3),
 - personenbezogene Daten aus Feedcube in Supportanfragen (Abschnitt 2 Nr. 19); sie werden gelöscht oder anonymisiert.

- (2) Nutzt der Auftraggeber weitere Produkte des Auftragnehmers über das Ende des Hauptvertrags hinaus, löscht der Auftragnehmer statt der gesamten Datenbank des Mandanten die Daten von Feedcube, insbesondere Umfragen, Einladungen, Antworten, Fragen und Fragebögen. Benutzerkonten und gemeinsam genutzte Stammdaten, die für die weiter genutzten Produkte erforderlich sind, bleiben nach den gesonderten Ergänzungen zu diesen Produkten bestehen.
- (3) Aus den Datensicherungen scheiden die gelöschten Daten spätestens 3 Tage nach der Löschung aus (Abschnitt 2 Nr. 20). Daten in Server-Protokollen und bei Unterauftragsverarbeitern werden nach den Fristen in Abschnitt 2 gelöscht.
- (4) Der Auftragnehmer bestätigt die Löschung auf Anforderung schriftlich oder in elektronischer Form (z. B. E-Mail); § 11 Abs. 6 der Vereinbarung bleibt unberührt.