

Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO

zwischen

Unternehmenskunden der Plattform „FASTCUBE Fixture Builder“

als Verantwortlicher

– nachfolgend „**Auftraggeber**“ genannt –

und

CENIT AG

Industriestraße 52-54

70565 Stuttgart

Deutschland

als Auftragsverarbeiter

– nachfolgend „**Auftragnehmer**“ genannt –

Auftraggeber und Auftragnehmer jeweils auch als „**Partei**“ und zusammen als „**Parteien**“ bezeichnet.

Präambel

Der Auftraggeber hat den Auftragnehmer mit den in Ziffer 1 genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten, für die der Auftraggeber als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DSGVO gilt. Dieser Auftragsverarbeitungsvereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 Abs. 3 Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit dem Umgang des Auftragnehmers oder von ihm unterbeauftragte Dritte mit personenbezogenen Daten des Auftraggebers zur Durchführung des Hauptvertrages.

Es werden die Begriffsdefinitionen der DSGVO zugrunde gelegt.

Inhaltsverzeichnis

1.	Vertragsgegenstand und Dauer	2
2.	Beschreibung der Verarbeitung	2
3.	Weisungsrecht	3
4.	Pflichten des Auftragnehmers	3
5.	Technische und organisatorische Sicherheitsmaßnahmen	5
6.	Kontrollrechte des Auftraggebers	5
7.	Einsatz von Unterauftragsverarbeitern	6
8.	Internationale Datenübermittlung	7
9.	Löschung von Auftraggeber-Daten	8
10.	Haftung	8
11.	Schlussbestimmungen	8

1. Vertragsgegenstand und Dauer

- 1.1 Der Auftragnehmer erbringt für den Auftraggeber folgende Leistungen auf Grundlage der Vereinbarung („Hauptvertrag“) im Zusammenhang mit der Erbringung von Cloud-/SaaS-Leistungen, insbesondere zur Bereitstellung von browserbasierten SaaS-Anwendungen zur automatisierten Vorrichtungskonstruktion.

Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

- 1.2 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

- 1.3 Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet (nachfolgend „**Auftraggeber-Daten**“ genannt) werden.

- 1.4 Die Daten werden vom Auftragnehmer nur für die Anlage 1 angegebene Dauer verarbeitet.

2. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten sowie Kategorien der von der Verarbeitung betroffenen Personen und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anlage 1** aufgeführt. Im Übrigen ergeben

sich Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer aus dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung).

3. Weisungsrecht

- 3.1 Der Auftragnehmer darf Auftraggeber-Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Von dieser Mitteilungspflicht darf der Auftragnehmer nur absehen, soweit und solange das betreffende Recht eine solche Information wegen eines wichtigen öffentlichen Interesses ausdrücklich verbietet.
- 3.2 Die Weisungen des Auftraggebers werden anfänglich durch den Hauptvertrag und diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung datenschutzrechtlicher Weisungen berechtigt, sofern die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer betroffen ist. Dies umfasst insbesondere Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Auftraggeber-Daten sowie auf die in Zusammenhang mit der Verarbeitung der Auftraggeber-Daten vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen.
- 3.3 Alle erteilten Weisungen sind vom Auftraggeber zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
- 3.4 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

4. Pflichten des Auftragnehmers

- 4.1 Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
- 4.2 Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter bestellt:

intersoft consulting services AG

Beim Strohhouse 17

20097 Hamburg

Tel.: +49 711 7825-30
Fax: +49 711 7825-4000
E-Mail: datenschutzbeauftragter@cenit.com

- 4.3 Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend „**eingesetzte Personen**“ genannt), entsprechend zur Vertraulichkeit verpflichten, es sei denn sie unterliegen bereits einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung, (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus dieser Vereinbarung ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der Verpflichtung sicherstellen.
- 4.4 Der Auftragnehmer wird angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Betroffenenrechte unterstützen. Sollte sich ein Betroffener direkt den Auftragnehmer wenden, um die Betroffenenrechte erkennbar hinsichtlich der im Auftrag des Auftraggebers verarbeiteten Auftraggeber-Daten wahrzunehmen, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftraggeber wird dem Auftragnehmer den insoweit entstehenden Aufwand vergüten, sofern und soweit nach anwendbarem Datenschutzrecht zulässig.
- 4.5 Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der in Art. 32-36 DS-GVO genannten Pflichten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden. Der Auftraggeber wird den Auftragnehmer den insoweit entstehenden Aufwand vergüten, sofern und soweit nach anwendbarem Datenschutzrecht zulässig.
- 4.6 Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer, den im Rahmen des Auftrags eingesetzten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber in angemessener Frist informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes der Auftraggeber-Daten enthält, soweit möglich, folgende Informationen:
- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
 - b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

- c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen. Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Auftraggeber-Daten von einer Verletzung nach Satz 1 betroffen sind.

- 4.7 Der Auftragnehmer wird dem Auftraggeber die für die Führung des Verzeichnisses der Verarbeitungstätigkeiten notwendigen Informationen zur Verfügung stellen.

5. Technische und organisatorische Sicherheitsmaßnahmen

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in **Anlage 2** aufgeführten Sicherheitsmaßnahmen, getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Sicherheitsmaßnahmen anfordern. Über wesentliche Änderungen der Sicherheitsmaßnahmen hat der Auftragnehmer den Auftraggeber in Textform zu unterrichten.

6. Kontrollrechte des Auftraggebers

- 6.1 Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in diesem Vertrag niedergelegten Pflichten durch den Auftragnehmer, insbesondere der technischen und organisatorischen Maßnahmen. Auf Verlangen des Auftraggebers gestattet der Auftragnehmer ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Auftraggeber einschlägige Zertifizierungen des Auftragnehmers berücksichtigen.
- 6.2 Der Auftraggeber kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragnehmers umfassen und werden gegebenenfalls mit angemessener Vorankündigung, wenn dadurch der Zweck der Überprüfung

gefährdet würde, durchgeführt. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

- 6.3 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der Einhaltung der in diesem Vertrag niedergelegten Pflichten sowie der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind und Vor-Ort-Kontrollen zuzulassen.
- 6.4 Der Auftraggeber trägt jegliche Kosten für Kontrollen, es sei denn, eine solche Kontrolle deckt eine wesentliche Verletzung der Vereinbarung durch den Auftragnehmer auf; in diesen Fällen trägt der Auftragnehmer die eigenen Kosten der Kontrolle. Falls sich aus einer Kontrolle ergibt, dass der Auftragnehmer seinen Verpflichtungen aus der Vereinbarung nicht nachgekommen ist, heilt der Auftragnehmer diese Verletzung in angemessener Frist auf eigene Kosten.

7. Einsatz von Unterauftragsverarbeitern

- 7.1 Der Auftragnehmer besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern, die in der dieser Vereinbarung als **Anlage 3** beigefügten Liste aufgeführt sind. Der Auftragnehmer unterrichtet den Auftraggeber mindestens vier (4) Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Auftraggeber damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Wenn der Auftraggeber nicht innerhalb der Frist von vier (4) Wochen widerspricht, gilt der neue Unterauftragsverarbeiter als vom Auftraggeber akzeptiert.
- 7.2 Wenn der Auftraggeber gemäß dem Datenschutzrecht einen berechtigten Grund hat, gegen die Verarbeitung Personenbezogener Daten durch die/den neuen Unterauftragsverarbeiter zu widersprechen, kann der Auftraggeber die Vereinbarung (beschränkt auf die Leistung, für den der neue Unterauftragsverarbeiter eingesetzt werden soll) durch schriftliche Mitteilung an den Auftragnehmer kündigen. Diese Kündigung tritt zu dem vom Auftraggeber festgelegten Zeitpunkt in Kraft, spätestens aber mit Übernahme der Leistungen durch den neuen Unterauftragsverarbeiter.
- 7.3 Beauftragt der Auftragnehmer einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des verantwortlichen Auftraggebers), so muss diese Beauftragung im Wege eines Untervergabevertrags erfolgen, der dem Unterauftragsverarbeiter dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragnehmer gemäß dieser Vereinbarung gelten. Der Auftragnehmer gewährleistet, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der

Auftragnehmer entsprechend diesen Klauseln und gemäß der DSGVO unterliegt. Der Auftragnehmer sorgt dafür, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Unterauftragsverarbeitern wahrnehmen kann. Der Auftragnehmer ist verpflichtet, Unterauftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen

- 7.4 Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Auftraggebers.
- 7.5 Eine Unterauftragsverarbeitung im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Unterauftragsverhältnisse dar, die den Regelungen dieser Ziffer 7 unterliegen, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

8. Internationale Datenübermittlung

- 8.1 Der Auftragnehmer wird Auftraggeber-Daten, die im Rahmen dieser Vereinbarung verarbeitet werden, nicht in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) übermitteln oder dort verarbeiten lassen, für das kein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 Abs. 3 DSGVO besteht („unsicherer Drittstaat“), es sei denn, eine solche Übermittlung ist nach Maßgabe der Art. 44 ff. DSGVO zulässig.
- 8.2 Ist der Auftragnehmer aufgrund des Rechts der Europäischen Union oder eines Mitgliedstaats, dem er unterliegt, verpflichtet, Auftraggeber-Daten an einen unsicheren Drittstaat zu übermitteln, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor Durchführung der Übermittlung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.
- 8.3 Eine Übermittlung von Auftraggeber-Daten in einen unsicheren Drittstaat ist insbesondere zulässig, wenn eine geeignete Garantie im Sinne des Art. 46 DSGVO gegeben ist, insbesondere durch:
 - a) den Abschluss der jeweils gültigen Standardvertragsklauseln der EU-Kommission (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO,
 - b) verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCR) gemäß Art. 47 DSGVO, oder
 - c) einen sonstigen zulässigen Übermittlungsmechanismus nach Art. 46 DSGVO.
- 8.4 Sofern Standardvertragsklauseln oder Binding Corporate Rules eingesetzt werden, stellt der Auftragnehmer sicher, dass

- vor der Übermittlung eine Bewertung der Rechtslage und Praxis im Drittstaat (Transfer-Impact-Assessment) erfolgt und
- gegebenenfalls zusätzliche technische und organisatorische Maßnahmen implementiert werden, um ein der DSGVO im Wesentlichen gleichwertiges Schutzniveau sicherzustellen.

8.5 Der Einsatz von Unterauftragsverarbeitern in einem unsicheren Drittstaat ist nur zulässig, wenn

- der betreffende Unterauftragsverarbeiter ordnungsgemäß gemäß dieser Vereinbarung genehmigt wurde,
- die Voraussetzungen der Art. 28 Abs. 2 und 4 DSGVO erfüllt sind und
- die Anforderungen der Art. 44 ff. DSGVO eingehalten werden, insbesondere durch entsprechende vertragliche Garantien

9. Löschung von Auftraggeber-Daten

9.1 Nach Abschluss der vertragsgegenständlichen Verarbeitungsleistungen oder mit Ablauf der Laufzeit dieser Vereinbarung wird der Auftragnehmer nach Wahl des Auftraggebers alle ihm überlassenen personenbezogenen Daten entweder löschen oder an den Auftraggeber zurückgeben, sofern und soweit nicht nach dem Recht der Europäischen Union oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht.

9.2 Die vorstehende Verpflichtung erstreckt sich auch auf etwaige beim Auftragnehmer vorhandene Datensicherungen. Gesetzliche Aufbewahrungspflichten bleiben unberührt; für deren Dauer sind die betreffenden Daten in der Verarbeitung zu sperren und ausschließlich zu den gesetzlich vorgeschriebenen Zwecken zu verarbeiten.

9.3 Der Auftragnehmer wird dem Auftraggeber die vertragsgemäße Löschung oder Rückgabe der Daten auf Verlangen in geeigneter Weise nachweisen.

10. Haftung

Auf Art. 82 DS-GVO wird verwiesen. Im Übrigen wird vereinbart, dass die Regelungen zur Haftungsbeschränkung aus dem Hauptvertrag gelten sollen.

11. Schlussbestimmungen

11.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

11.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Schriftform oder eines dokumentierten elektronischen Formats.

11.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

11.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Folgende Dokumente sind untrennbarer Bestandteil dieser Vereinbarung:

Anlage 1: Beschreibung der Verarbeitung

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Anlage 3: Unterauftragsverhältnisse beim Auftragnehmer

Auftraggeber

Auftragnehmer

(Ort/Datum)

(Ort/Datum)

(Unterschrift)

(Unterschrift)

Anlage 1:

Beschreibung der Verarbeitung

I. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- | | |
|--|--|
| ☒ Interessenten | Besucher der Plattform, Registrierungsinteressenten, Unternehmen im Verifizierungsprozess, |
| ☒ Kunden | Geschäftskunden der FASTCUBE-Plattform, Nutzer (Member, Admin, Owner) mit oder ohne aktive Subscription, Beschäftigte und sonstige Nutzer von Unternehmenskunden |
| ☒ Nutzer | Nutzer der FASTCUBE-Plattform, Nutzer des Kundenportals, Support-Anfragende |

II. Kategorien personenbezogener Daten, die verarbeitet werden

- | | |
|--|--|
| ☒ Personenstammdaten | Vor- und Nachname, Unternehmenszugehörigkeit, Nutzerrolle (z. B. Owner, Member, Maker, Viewer) |
| ☒ Adressdaten | Unternehmensanschrift, Land, Ort, Postleitzahl |
| ☒ Kontakt Daten | Geschäftliche E-Mail-Adresse, Telefonnummer, Ansprechpartnerdaten |
| ☒ Zahlungs-/Bankdaten | Rechnungsanschrift, USt-IdNr., Zahlungs- und Transaktionsdaten, Bestell- und Abonnementinformationen, von Stripe verarbeitete Zahlungsinformationen |
| ☒ Technische Daten | IP-Adresse, Login- und Authentifizierungs-Daten, insbesondere Benutzerkennung, Microsoft-Entra-ID-Informationen, OTP-Informationen, Logfiles, insbesondere Datenbank-Abfrage, Time-Stamp, Login-Aktionen, vom Nutzer |

	bereitgestellte CAD-Daten und Projektdaten
☒ Protokolldateien, Geräteinformationen (Browser an Webserver)	Angeforderte URL (konkrete Seite), Zugriffsstatus/HTTP-Statuscode, übertragene Datenmenge, Website von der die Anforderung kommt (Referrer-URL), Browser-Typ, Browser-Spracheinstellung
☒ Support- und Kommunikationsdaten	Inhalte von Supportanfragen, Ticketinformationen, E-Mail-Kommunikation, Dokumentationen von Support- und Fernwartungsvorgängen; Daten, die im Rahmen von Fernwartungs- oder Supportleistungen (z. B. TeamViewer) eingesehen oder verarbeitet werden können

III. Art der Verarbeitung

Erheben, Erfassen, Speichern, Auslesen, Abfragen, Verwenden, Übermitteln (an Unterauftragnehmer Microsoft Azure, Stripe), Einschränken, Löschen und Vernichten von personenbezogenen Daten im Rahmen der Bereitstellung und des Betriebs der SaaS-Plattform „FASTCUBE Fixture Builder“ einschließlich Nutzerregistrierung, Authentifizierung, Nutzerverwaltung, Abonnementverwaltung und technischem Plattformbetrieb.

IV. Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Die Verarbeitung erfolgt zum Zweck der Bereitstellung, des Betriebs und der Verwaltung der SaaS-Plattform „FASTCUBE Fixture Builder“ für den Auftraggeber und dessen autorisierte Nutzer. Dies umfasst insbesondere:

- Registrierung und Verwaltung von Unternehmenskonten und Nutzerkonten
- Authentifizierung und Autorisierung der Nutzer
- Bereitstellung der Plattformfunktionalitäten (Projektanlage, Vorrichtungserstellung, Datenexport)
- Verwaltung von Subscriptions und Lizenzzuweisungen
- Technischer Betrieb, Fehleranalyse und Sicherstellung der IT-Sicherheit
- Kommunikation mit Nutzern (Systembenachrichtigungen, Supportanfragen)

V. Dauer der Verarbeitung

Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages

Anlage 2:

Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Nachfolgend sind die technischen und organisatorischen Maßnahmen beschrieben, die der Auftragnehmer unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen ergriffen hat.

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1. Zutrittskontrolle

Der Auftragnehmer ergreift Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Rechenzentren (Verarbeitung der Auftraggeber-Daten)

Der Auftragnehmer betreibt keine eigenen Rechenzentren für die Erbringung der vertragsgegenständlichen Leistungen. Die Verarbeitung erfolgt in Rechenzentren der Microsoft Ireland Operations Ltd. in der Azure-Region „Germany West Central“ (Frankfurt am Main, Deutschland). Der physische Zutritt wird dort durch folgende Maßnahmen des Unterauftragsverarbeiters sichergestellt:

- Mehrstufiges Zutrittskontrollsystem mit Perimetersicherung, Vereinzelungsanlagen und personalisierten Zutrittsmedien
- Biometrische Authentifizierung in sicherheitsrelevanten Zonen
- Rund um die Uhr besetzter Sicherheitsdienst und Videoüberwachung der Zutrittspunkte und Außenbereiche
- Zutritt ausschließlich nach dokumentierter Genehmigung und nach dem Need-to-know-Prinzip, zeitlich begrenzt und rollenbezogen
- Protokollierung sämtlicher Zutritte einschließlich Besucherbegleitung
- Zertifizierter Nachweis über ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 sowie SOC 1 und SOC 2 Type II Prüfberichte

Der Auftragnehmer prüft die Wirksamkeit dieser Maßnahmen anhand der vom Unterauftragsverarbeiter bereitgestellten Zertifikate und Prüfberichte und stellt diese dem Auftraggeber auf Anforderung zur Verfügung.

Standorte des Auftragnehmers (Administration und Support)

- Zutritt zum Betriebsgelände und zu Bürobereichen ausschließlich über personalisierte, elektronisch protokollierte Zutrittsausweise
- Besetzter Empfang während der Geschäftszeiten, Besucher werden registriert und begleitet

- Technik- und Netzwerkräume sind gesondert verschlossen und nur einem festgelegten Personenkreis zugänglich
- Dokumentierter Prozess zur Ausgabe, Sperrung und Rückgabe von Zutrittsmedien bei Ein- und Austritt von Beschäftigten
- Verpflichtende Clean-Desk- und Clear-Screen-Regelung
- Datenschutzgerechte Vernichtung physischer Datenträger und Unterlagen nach DIN 66399

1.2. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden.

Zugang der Nutzer des Auftraggebers zur Plattform

- Authentifizierung ausschließlich über Microsoft Entra ID; die Verarbeitung der Identitäts- und Authentifizierungsdaten erfolgt in der Azure-Geolokation „Europe“
- Nutzer mit eigenem Entra-ID-Tenant authentifizieren sich über Föderation, so dass die Zugangsrichtlinien des Auftraggebers einschließlich Multi-Faktor-Authentifizierung und Conditional Access unmittelbar wirken.
- Nutzer ohne Microsoft-Konto authentifizieren sich über ein zeitlich befristetes, an die geschäftliche E-Mail-Adresse gesendetes Einmalpasswort (OTP); ein statisches Passwort wird für diesen Weg nicht vergeben
- Jedes Nutzerkonto ist personenbezogen; Sammel- oder Funktionskonten für Endnutzer sind nicht vorgesehen
- Automatische Sperrung nach einer definierten Anzahl fehlgeschlagener Anmeldeversuche sowie automatische Beendigung inaktiver Sitzungen
- Anmeldevorgänge, fehlgeschlagene Anmeldeversuche und sicherheitsrelevante Kontoänderungen werden protokolliert
- Nutzerkonten werden durch Nutzer mit der Rolle „Owner“ oder „Admin“ des Auftraggebers angelegt, geändert und deaktiviert; die Verantwortung für den zeitnahen Entzug bei Ausscheiden eines Nutzers liegt beim Auftraggeber

Zugang der Beschäftigten des Auftragnehmers zu den Systemen

- Administrative Zugriffe erfolgen ausschließlich über personalisierte, von den Standardkonten getrennte administrative Konten mit verpflichtender Multi-Faktor-Authentifizierung
- Zugang zur Produktivumgebung nur aus verwalteten Unternehmensgeräten über verschlüsselte Verbindungen; ein Zugriff aus dem offenen Internet ohne vorgelagerte Authentifizierung ist technisch ausgeschlossen.
- Zentral durchgesetzte Passwortsrichtlinie mit Vorgaben zu Mindestlänge, Komplexität und Sperrung kompromittierter Passwörter
- Endgeräte mit vollständiger Festplattenverschlüsselung, zentral verwalteter Endpoint-Protection und automatisiertem Patch-Management
- Dokumentierter Onboarding- und Offboarding-Prozess; Zugänge werden bei Ausscheiden unverzüglich gesperrt

- Netzsegmentierung sowie Filterung durch Firewalls und Network Security Groups; Datenbank- und Backend-Dienste sind nicht öffentlich erreichbar
- Sämtliche Übertragung erfolgt ausschließlich transportverschlüsselt über TLS in einer aktuellen Version

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können sowie, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Berechtigungskonzept innerhalb der Plattform

- Die Daten jedes Auftraggebers werden einem abgegrenzten Arbeitsbereich (Unternehmens-Tenant) zugeordnet. Ein Zugriff auf Daten anderer Auftraggeber ist technisch ausgeschlossen; jede Anfrage wird serverseitig gegen die Tenant-Zugehörigkeit des authentifizierten Nutzers geprüft
- Innerhalb des Unternehmenskontos gilt ein rollenbasiertes Berechtigungskonzept mit den Rollen „Owner“, „Admin“ und „Member“, das die administrativen Berechtigungen abstuft
- Der funktionale Umfang eines Nutzers wird zusätzlich über den zugewiesenen Lizenztyp („Maker“, „Viewer“) begrenzt
- Die Vergabe und der Entzug von Rollen und Lizenztypen erfolgen durch den Auftraggeber selbst über die Nutzerverwaltung der Plattform

Berechtigungen der Beschäftigten des Auftragnehmers

- Zugriffsrechte werden nach dem Need-to-know-Prinzip und dem Grundsatz der geringsten Rechte vergeben und sind an die jeweilige Rolle gebunden
- Ein Zugriff von Beschäftigten des Auftragnehmers auf Inhaltsdaten des Auftraggebers findet im Regelbetrieb nicht statt. Er erfolgt ausschließlich anlassbezogen zur Störungsbeseitigung oder auf Anforderung des Auftraggebers, wird auf den erforderlichen Umfang begrenzt und protokolliert
- Fernzugriffe im Rahmen des Supports mittels TeamViewer oder vergleichbarer Werkzeuge erfolgen ausschließlich nach vorheriger Zustimmung des Auftraggebers und unter dessen Beobachtung
- Beantragung, Genehmigung und Entzug von Berechtigungen erfolgen in einem dokumentierten Verfahren; die Berechtigungen privilegierter Konten werden mindestens jährlich überprüft
- Administrative Tätigkeiten in der Produktivumgebung werden protokolliert; die Protokolle sind gegen Veränderung durch die protokollierten Personen geschützt
- Alle eingesetzten Personen sind auf die Vertraulichkeit verpflichtet und im Datenschutz unterwiesen

Schutz gespeicherter Daten

- Sämtliche gespeicherten personenbezogenen Daten werden im Ruhezustand mittels AES-256 verschlüsselt. Dies umfasst insbesondere Datenbanken, Objektspeicher sowie persistente Speichervolumen der in Microsoft Azure betriebenen Kubernetes-Plattform. Die Verschlüsselung erfolgt auf Ebene der Azure-Speicher- und Datenbankdienste.
- Verwaltung kryptografischer Schlüssel über Azure Key Vault mit rollenbasiertem Berechtigungskonzept.
- Trennung von Produktiv-, Staging- und Entwicklungsumgebungen.
- Vernichtung von Datenträgern in den Rechenzentren des Unterauftragsverarbeiters nach NIST SP 800-88

1.4. Datentrennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Trennung zwischen Auftraggebern (Mandantentrennung)

- Sämtliche Projekte, Nutzerkonten und Arbeitsergebnisse werden logisch einem Unternehmens-Tenant zugeordnet. Die Tenant-Kennung ist Pflichtbestandteil jedes Datensatzes
- Die Zuordnung wird serverseitig bei jeder Anfrage gegen die Tenant-Zugehörigkeit des authentifizierten Nutzers geprüft. Die Prüfung erfolgt in der Anwendungslogik und nicht in der Oberfläche, ein Umgehen über direkte Schnittstellenaufrufe ist damit ausgeschlossen
- Objektspeicher für Werkstückmodelle und Exportdateien werden je Tenant in getrennten Pfaden mit eigenständigen Zugriffsrichtlinien geführt
- Die Wirksamkeit der Mandantentrennung wird bei jeder Änderung an Datenzugriffspfaden durch automatisierte Tests überprüft

Trennung nach Verarbeitungszweck

- Identitäts- und Authentifizierungsdaten werden in Microsoft Entra ID verarbeitet und dort ausschließlich zum Zweck der Authentifizierung und ob dem Nutzer eine Maker Lizenz zugeordnet ist.
- Zahlungs- und Abrechnungsdaten werden beim Unterauftragsverarbeiter Stripe Payments Europe Ltd. verarbeitet. In der Plattform selbst werden keine vollständigen Zahlungsdaten gespeichert, sondern ausschließlich Referenzkennungen.
- Technische Protokoll- und Betriebsdaten werden getrennt von den Anwendungsdaten gespeichert, mit eigenem Berechtigungskonzept und eigener Aufbewahrungsfrist
- Produktiv-, Test- und Entwicklungsumgebungen sind vollständig getrennt betrieben. Produktivdaten werden nicht in Test- oder Entwicklungsumgebungen übernommen

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die vertragsgegenständliche Verarbeitung erfordert die Identifizierbarkeit der Nutzer, da Authentifizierung, Rollenzuweisung, Lizenzzuordnung und Zurechnung von Projektänderungen personenbezogen erfolgen müssen. Eine vollständige Pseudonymisierung

des Produktivbetriebs ist daher nicht möglich. Der Auftragnehmer ergreift folgende Maßnahmen:

- Datenanalysen zu Produktnutzung, Fehlerhäufigkeit und Kapazitätsplanung erfolgen ausschließlich auf aggregierten oder pseudonymisierten Datenbeständen ohne Rückschluss auf einzelne Nutzer
- In Test- und Entwicklungsumgebungen werden ausschließlich synthetische oder anonymisierte Datensätze verwendet
- Personenbezogene Kennungen werden in internen Auswertungen durch technische Kennungen ohne Klarnamen ersetzt; die Zuordnungstabelle unterliegt einem gesonderten Berechtigungskonzept
- Bei der Weitergabe von Protokolldaten an Dritte zur Fehleranalyse werden personenbezogene Merkmale vor der Übermittlung entfernt oder ersetzt

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Schutz während der Übertragung

- Sämtliche Verbindungen zwischen dem Browser des Nutzers und der Plattform erfolgen ausschließlich über TLS in einer aktuellen Version. Unverschlüsselte Verbindungen werden serverseitig abgewiesen und auf die verschlüsselte Variante umgeleitet
- HTTP Strict Transport Security ist aktiviert; veraltete Protokollversionen und schwache Cipher Suites sind deaktiviert
- Die Kommunikation zwischen den Diensten der Plattform erfolgt innerhalb eines geschlossenen, nicht öffentlich erreichbaren Netzwerks in Microsoft Azure. Verbindungen zu Datenbank- und Speicherdiensten sind ebenfalls transportverschlüsselt
- Administrative Zugriffe erfolgen ausschließlich über verschlüsselte Verbindungen von verwalteten Unternehmensgeräten

Dokumentation der Übermittlungswege

- Sämtliche vorgesehenen Empfänger personenbezogener Daten sind abschließend in Anlage 3 dieser Vereinbarung dokumentiert. Über diese Empfänger hinaus findet keine Übermittlung statt
- Zweck, Umfang und Ort der Leistungserbringung sind je Empfänger festgehalten; Änderungen unterliegen dem Verfahren nach Ziffer 7 dieser Vereinbarung
- Der Export von Arbeitsergebnissen durch den Auftraggeber (.DXF, .STEP) erfolgt über die verschlüsselte Verbindung der Anwendung und wird protokolliert
- Eine Übermittlung in Drittländer ohne Angemessenheitsbeschluss findet nicht statt

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Jede Aktion in der Plattform erfolgt unter einer personenbezogenen Nutzerkennung. Anonyme oder unter Sammelkonten ausgeführte Verarbeitungen sind nicht vorgesehen
- Anlage, Änderung und Löschung von Nutzerkonten, Zuweisung und Entzug von Rollen sowie Zuweisung und Entzug von Lizenztypen werden mit Zeitstempel, auslösendem Nutzer und Art der Änderung protokolliert
- Anmeldungen, fehlgeschlagene Anmeldeversuche und Änderungen an Authentifizierungsmerkmalen werden in Microsoft Entra ID protokolliert
- Änderungen an Projekten und Vorrichtungen werden dem jeweils bearbeitenden Nutzerkonto zugeordnet und mit Bearbeitungszeitpunkt gespeichert
- Administrative Eingriffe in die Produktivumgebung durch Beschäftigte des Auftragnehmers werden gesondert protokolliert
- Protokolldaten werden schreibgeschützt in einem getrennten Speicherbereich abgelegt. Die protokollierten Personen haben keine Berechtigung, die sie betreffenden Protokolleinträge zu ändern oder zu löschen
- Die Aufbewahrungsdauer der Protokolldaten ist festgelegt; nach Ablauf erfolgt eine automatisierte Löschung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Betrieb in Microsoft Azure, Region „Germany West Central“, mit redundanter Auslegung der Speicher- und Datenbankdienste über mehrere physisch getrennte Standorte innerhalb der Region
- Redundante Auslegung der Rechenzentrumsinfrastruktur durch den Unterauftragsverarbeiter, insbesondere unterbrechungsfreie Stromversorgung, Netzersatzanlagen, redundante Klimatisierung sowie Brandfrüherkennung und Löschanlagen
- Betrieb der Anwendung in einer Container-Orchestrierung mit automatischem Neustart und Neuverteilung ausgefallener Instanzen
- Regelmäßige, automatisierte Sicherung der Datenbank- und Objektspeicherbestände; die Sicherungen sind verschlüsselt und getrennt vom Produktivbestand abgelegt
- Kontinuierliche Überwachung von Verfügbarkeit, Auslastung und Fehlerraten mit automatisierter Alarmierung an einen definierten Bereitschaftskreis
- Schutz vor Überlastung durch vorgelagerte Filterung, Ratenbegrenzung und Schutzmechanismen gegen verteilte Überlastangriffe
- Zentral verwaltete Schadsoftwareerkennung auf allen Endgeräten sowie automatisiertes Patch- und Schwachstellenmanagement für die Plattformkomponenten

- Die vertraglich geschuldete Verfügbarkeit der Plattform richtet sich nach der Leistungsbeschreibung zum Hauptvertrag

3.2. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.

- Dokumentiertes Sicherungs- und Wiederherstellungskonzept mit festgelegten Zielwerten für den maximal tolerierbaren Datenverlust (Recovery Point Objective) und die maximal tolerierbare Ausfalldauer (Recovery Time Objective)
- Punktgenaue Wiederherstellung der Datenbankbestände innerhalb des definierten Aufbewahrungszeitraums der Sicherungen
- Regelmäßige Überprüfung der Wiederherstellbarkeit durch Testwiederherstellungen; die Ergebnisse werden dokumentiert
- Vollständig automatisierte, versionierte Bereitstellung der Anwendungsumgebung, so dass die Betriebsumgebung reproduzierbar neu aufgebaut werden kann
- Dokumentierter Notfallplan mit definierten Rollen, Eskalationswegen und Erreichbarkeiten
- Der Auftraggeber bleibt für eine ausreichende eigene Sicherung seiner Anwendungsdaten verantwortlich; die Sicherungen des Auftragnehmers dienen der Wiederherstellung des Systembetriebs und ersetzen keine Datensicherung des Auftraggebers

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Datenschutz-Management

- Bestellung eines externen betrieblichen Datenschutzbeauftragten (intersoft consulting services AG, Hamburg), erreichbar unter datenschutzbeauftragter@cenit.com
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO
- Verbindliche interne Datenschutzrichtlinien; alle eingesetzten Personen sind nach Art. 28 Abs. 3 lit. b DSGVO zur Vertraulichkeit verpflichtet
- Regelmäßige, mindestens jährliche Schulung und Sensibilisierung der eingesetzten Personen zu Datenschutz und Informationssicherheit
- Datenschutzrechtliche Prüfung neuer oder geänderter Verarbeitungstätigkeiten vor deren Einführung, einschließlich Prüfung der Erforderlichkeit einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO
- Dokumentiertes Verfahren zur Auswahl, Prüfung und Überwachung von Unterauftragsverarbeitern einschließlich Auswertung vorgelegter Zertifikate und Prüfberichte
- Regelmäßige Überprüfung und Aktualisierung der in dieser Anlage beschriebenen Maßnahmen, mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitung
- Dokumentiertes Verfahren zur Bearbeitung von Betroffenenanfragen nach Art. 15 bis 22 DSGVO einschließlich Unterstützung des Auftraggebers nach Ziffer 4 dieser Vereinbarung

4.2. Incident-Response-Management

Maßnahmen bei der Reaktion auf Sicherheitsverletzungen.

- Dokumentierter Prozess zur Erkennung, Meldung, Bewertung und Behandlung von Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten
- Zentrale Meldestelle für Sicherheitsvorfälle; alle eingesetzten Personen sind verpflichtet, Verdachtsfälle unverzüglich zu melden
- Technische Erkennung durch fortlaufende Überwachung, Alarmierung bei sicherheitsrelevanten Ereignissen und Auswertung der Protokolldaten
- Festgelegte Rollen, Eskalationsstufen und Erreichbarkeiten für die Vorfallobearbeitung, einschließlich Einbindung des Datenschutzbeauftragten
- Bewertung jedes Vorfalls hinsichtlich Meldepflicht nach Art. 33 DSGVO und Benachrichtigungspflicht nach Art. 34 DSGVO
- Unverzügliche Information des Auftraggebers bei Verletzungen des Schutzes personenbezogener Daten, die Auftraggeber-Daten betreffen, unter Angabe der Art der Verletzung, der betroffenen Datenkategorien, der wahrscheinlichen Folgen sowie der ergriffenen und vorgeschlagenen Maßnahmen
- Dokumentation aller Vorfälle einschließlich Ursachenanalyse und abgeleiteter Korrekturmaßnahmen
- Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von dessen Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und den betroffenen Personen

4.3. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

- Datenminimierung bei der Registrierung: erhoben werden ausschließlich die für Vertragsabwicklung, Authentifizierung und Betrieb erforderlichen Daten
- Der Umfang der in der Plattform verarbeiteten personenbezogenen Daten wird durch den Auftraggeber bestimmt. Eine Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO ist nicht vorgesehen
- Neue Nutzer erhalten in der Voreinstellung die Rolle „Member“ und den Lizenztyp „Viewer“, also den geringsten Berechtigungsumfang. Erweiterte Berechtigungen müssen aktiv durch den Auftraggeber zugewiesen werden
- Kein Zugriff der Beschäftigten des Auftragnehmers auf Inhaltsdaten im Regelbetrieb; Zugriffe erfolgen ausschließlich anlassbezogen und protokolliert
- Fernwartungszugriffe im Rahmen des Supports setzen die vorherige Zustimmung des Auftraggebers voraus
- Datenschutzerfordernisse sind fester Bestandteil des Entwicklungsprozesses; sicherheitsrelevante Änderungen unterliegen einer Prüfung durch eine zweite Person vor Übernahme in die Produktivumgebung
- Festgelegte Löschfristen: nach Löschung des Unternehmenskontos werden sämtliche Kundendaten nach Ablauf von 30 Kalendertagen unwiderruflich gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen
- Der Auftraggeber verwaltet Nutzerkonten, Rollen und Lizenzzuweisungen eigenständig und kann Zugänge jederzeit selbst entziehen

4.4. Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Schriftlicher Auftragsverarbeitungsvertrag nach Art. 28 DSGVO mit eindeutiger Festlegung von Gegenstand, Dauer, Art, Zweck und Umfang der Verarbeitung in Anlage 1
- Verpflichtung aller eingesetzten Personen auf Vertraulichkeit und auf die Einhaltung der Weisungsbindung sowie Belehrung über die sich aus dieser Vereinbarung ergebenden Datenschutzpflichten
- Dokumentiertes Verfahren zur Entgegennahme, Prüfung und Umsetzung von Einzelweisungen des Auftraggebers; benannte weisungsbefugte und weisungsempfangende Ansprechpartner
- Prüfung eingehender Weisungen auf datenschutzrechtliche Zulässigkeit; bei erkennbarem Verstoß erfolgt eine unverzügliche Mitteilung an den Auftraggeber nach Ziffer 3 dieser Vereinbarung
- Keine Verarbeitung zu eigenen Zwecken des Auftragnehmers; insbesondere keine Nutzung der Auftraggeber-Daten für eigene Analysen, Werbung oder das Training von Modellen
- Sorgfältige Auswahl der Unterauftragsverarbeiter nach Eignung und Zuverlässigkeit; vertragliche Weitergabe derselben Datenschutzpflichten und Weisungsbindung, dokumentiert in Anlage 3
- Regelmäßige Überprüfung der Unterauftragsverarbeiter anhand vorgelegter Zertifikate und Prüfberichte
- Ermöglichung von Kontrollen und Audits durch den Auftraggeber nach Ziffer 6 dieser Vereinbarung, einschließlich Bereitstellung der erforderlichen Auskünfte und Nachweise
- Nachweis der weisungsgemäßen Löschung oder Rückgabe der Auftraggeber-Daten nach Vertragsende auf Verlangen des Auftraggebers

Anlage 3:

Unterauftragsverhältnisse beim Auftragnehmer

Unterauftragnehmer (Firmenname mit Rechtsform)	Beschreibung der (Teil-)Leistungen	Anschrift/ Ort der Leistungserbringung	Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO
Stripe Payments Europe Limited	Zahlungsabwicklung	One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Irland	Transfer ausschließlich in Staaten mit Angemessenheitsbeschluss oder Data Privacy Framework-zertifizierte Unternehmen oder unter Verwendung der EU- Standardvertragsklauseln (SCC).
Microsoft Ireland Operations Ltd.	Bereitstellung der Cloud-Infrastruktur (Azure) für Betrieb, Speicherung und Authentifizierung (Microsoft Entra ID)	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland; Ort der Verarbeitung: Azure-Region „Germany West Central“ (Frankfurt am Main, Deutschland), Entra ID: Azure- Geolokation „Europe“	Verarbeitung innerhalb der EU/des EWR; keine Übermittlung in unsichere Drittstaaten. Nachweise: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1 und SOC 2 Type II