CrayssnLabs GmbH
Kartäuserstraße 21d
99084 Erfurt

Handelsregister: HRB 524277
Registergericht: Amtsgericht Jena
GF: Sebastian Ludwig, Oliver Wiegler

Tel: +49 361 23002016
Mail: info@cl.team
Web: www.crayssnlabs.de

AUFTRAGSVERARBEITUNGSVEREINBARUNG (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

CrayssnLabs GmbH
Kartäuserstraße 21d
99084 Erfurt

(im Folgenden „Auftragnehmer“)

und

_____

(im Folgenden „Auftraggeber“)

wird folgende Vereinbarung geschlossen.

Diese Vereinbarung gilt ausschließlich in Verbindung mit einem zwischen den Vertragsparteien geschlossenen Hauptvertrag.

Version 1.0
Stand: August 2026

Inhalt

§1 Gegenstand der Vereinbarung

(1) Diese Vereinbarung regelt die Rechte und Pflichten der Vertragsparteien hinsichtlich der Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO).

(2) Sie ergänzt den zwischen den Parteien geschlossenen Hauptvertrag über die Erbringung von IT-Dienstleistungen. Soweit diese Vereinbarung abweichende datenschutzrechtliche Regelungen enthält, gehen diese den Bestimmungen des Hauptvertrages vor.

(3) Diese Vereinbarung findet ausschließlich Anwendung, soweit der Auftragnehmer im Rahmen der vereinbarten Leistungen personenbezogene Daten im Auftrag des Auftraggebers als Auftragsverarbeiter im Sinne des Art. 28 DSGVO verarbeitet.

(4) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit gesetzliche Vorschriften keine abweichende Verarbeitung vorschreiben.

§2 Dauer und Gegenstand der Verarbeitung

(1) Diese Vereinbarung gilt für sämtliche Verarbeitungen personenbezogener Daten, die der Auftragnehmer im Rahmen des zwischen den Parteien bestehenden Hauptvertrages als Auftragsverarbeiter gemäß Art. 28 DSGVO durchführt.

(2) Die Verarbeitung erfolgt ausschließlich zur Erfüllung der im Hauptvertrag vereinbarten Leistungen sowie der hierzu erforderlichen Nebenleistungen.

(3) Art, Zweck und Umfang der Verarbeitung, die Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen ergeben sich aus **Anlage 1** dieser Vereinbarung.

(4) Diese Vereinbarung tritt mit Abschluss des Hauptvertrages in Kraft und endet automatisch mit dessen Beendigung, sofern keine gesetzlichen Aufbewahrungspflichten oder sonstigen gesetzlichen Verpflichtungen einer Löschung oder Rückgabe der Daten entgegenstehen.

§3 Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisungen des Auftraggebers, soweit gesetzliche Vorschriften keine hiervon abweichende Verarbeitung verlangen.

(2) Weisungen können in Textform (z. B. per E-Mail oder über ein vereinbartes Ticketsystem) erteilt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Bis zur Klärung ist der Auftragnehmer berechtigt, die Ausführung der betreffenden Weisung auszusetzen, sofern die Aussetzung nicht selbst gegen gesetzliche Pflichten verstößt.

(4) Änderungen des Verarbeitungsgegenstandes oder wesentliche Änderungen der Verarbeitung bedürfen einer entsprechenden Weisung oder einer Anpassung des Hauptvertrages bzw. der **Anlage 1**.

§4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Hauptvertrages, dieser Vereinbarung sowie der dokumentierten Weisungen des Auftraggebers.

(2) Der Auftragnehmer gewährleistet, dass alle mit der Verarbeitung personenbezogener Daten befassten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung ihrer Tätigkeit fort.

(3) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die jeweils geltenden Maßnahmen ergeben sich aus **Anlage 2**.

(4) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen bei der Erfüllung seiner gesetzlichen Pflichten nach der DSGVO, insbesondere hinsichtlich

- der Wahrnehmung der Rechte betroffener Personen,
- der Sicherheit der Verarbeitung,
- der Meldung von Verletzungen des Schutzes personenbezogener Daten,
- der Datenschutz-Folgenabschätzung sowie
- einer gegebenenfalls erforderlichen Konsultation der zuständigen Aufsichtsbehörde.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn ihm Umstände bekannt werden, die gegen datenschutzrechtliche Vorschriften, diese Vereinbarung oder dokumentierte Weisungen des Auftraggebers verstoßen oder die Sicherheit der Verarbeitung beeinträchtigen können. Dies gilt auch für Anfragen oder Maßnahmen zuständiger Datenschutzaufsichtsbehörden, soweit diese die Verarbeitung personenbezogener Daten des Auftraggebers betreffen und eine Information rechtlich zulässig ist.

(6) Der Auftragnehmer führt die nach Art. 30 Abs. 2 DSGVO erforderlichen Verzeichnisse über die in seinem Verantwortungsbereich durchgeführten Verarbeitungstätigkeiten und stellt dem Auftraggeber auf berechtigtes Verlangen die zur Prüfung der Einhaltung dieser Vereinbarung erforderlichen Informationen zur Verfügung.

(7) Der Auftragnehmer setzt nur ausreichend qualifiziertes Personal ein und sorgt durch geeignete organisatorische Maßnahmen dafür, dass personenbezogene Daten ausschließlich im Rahmen der erteilten Berechtigungen verarbeitet werden.

(8) Der Auftragnehmer verarbeitet personenbezogene Daten nicht zu eigenen Zwecken und gibt diese nicht an Dritte weiter, sofern hierzu keine gesetzliche Verpflichtung besteht oder der Auftraggeber dies ausdrücklich angewiesen hat.

(9) Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO.

§5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten zu gewährleisten.

(2) Die technischen und organisatorischen Maßnahmen sind in **Anlage 2** zu dieser Vereinbarung beschrieben. Die Anlage ist Bestandteil dieser Vereinbarung.

(3) Der Auftragnehmer überprüft die technischen und organisatorischen Maßnahmen regelmäßig und passt sie unter Berücksichtigung des Stands der Technik sowie der tatsächlichen Risiken der Verarbeitung an.

(4) Änderungen der technischen und organisatorischen Maßnahmen sind zulässig, sofern das vereinbarte Schutzniveau nicht unterschritten wird und die Änderungen den Anforderungen der DSGVO entsprechen.

(5) Auf Verlangen des Auftraggebers weist der Auftragnehmer die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen in geeigneter Weise nach.

§ 6 Unterauftragnehmer

(1) Der Auftragnehmer ist berechtigt, zur Erfüllung seiner vertraglichen Leistungen weitere Auftragsverarbeiter (Unterauftragnehmer) einzusetzen.

(2) Der Auftragnehmer stellt sicher, dass jeder Unterauftragnehmer durch einen Vertrag gemäß Art. 28 DSGVO mindestens zu den Datenschutzpflichten verpflichtet wird, die auch gegenüber dem Auftraggeber bestehen.

(3) Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer ergeben sich aus **Anlage 3** dieser Vereinbarung.

(4) Beabsichtigt der Auftragnehmer die Beauftragung eines neuen Unterauftragnehmers oder eine wesentliche Änderung bestehender Unterauftragsverhältnisse, informiert er den Auftraggeber mindestens **14 Kalendertage** vor deren Wirksamwerden in Textform.

(5) Der Auftraggeber kann der beabsichtigten Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Im Falle eines berechtigten Widerspruchs werden die Vertragsparteien eine einvernehmliche Lösung anstreben. Kann keine Einigung erzielt werden, ist jede Partei berechtigt, den von der Änderung betroffenen Teil der Leistungen aus wichtigem Grund zu kündigen.

(6) Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der datenschutzrechtlichen Verpflichtungen seiner Unterauftragnehmer verantwortlich.

§ 7 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung der gesetzlichen Pflichten nach der DSGVO.

(2) Dies umfasst insbesondere die Unterstützung bei

a. der Wahrnehmung der Rechte betroffener Personen gemäß Art. 12 bis 22 DSGVO,

b. der Einhaltung der Anforderungen nach Art. 32 bis 36 DSGVO, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Meldung von Datenschutzverletzungen, der Benachrichtigung betroffener

Personen sowie der Durchführung von Datenschutz-Folgenabschätzungen und gegebenenfalls erforderlichen Konsultationen der zuständigen Aufsichtsbehörde.

(3) Gehen Anfragen betroffener Personen oder Datenschutzaufsichtsbehörden unmittelbar beim Auftragnehmer ein, informiert dieser den Auftraggeber unverzüglich und leitet die Anfrage an diesen weiter, sofern eine Weiterleitung rechtlich zulässig ist.

(4) Der Auftragnehmer beantwortet entsprechende Anfragen nicht eigenständig, es sei denn, er ist hierzu gesetzlich verpflichtet oder vom Auftraggeber ausdrücklich angewiesen worden.

(5) Unterstützungsleistungen, die über die vertraglich vereinbarten Leistungen hinausgehen und einen erheblichen zusätzlichen Aufwand verursachen, können gesondert vergütet werden, sofern dies vor ihrer Erbringung vereinbart wurde. Dies gilt nicht für Unterstützungsleistungen, die aufgrund eines vom Auftragnehmer zu vertretenden Verstoßes gegen diese Vereinbarung oder gegen datenschutzrechtliche Vorschriften erforderlich werden.

§ 8 Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DSGVO.

(2) Die Meldung erfolgt mindestens in Textform und enthält, soweit zum Zeitpunkt der Meldung bekannt, insbesondere folgende Informationen:

a. Art der Datenschutzverletzung,
b. Zeitpunkt oder Zeitraum der Datenschutzverletzung,
c. betroffene Verarbeitungsvorgänge oder IT-Systeme,
d. Kategorien und – soweit möglich – die ungefähre Anzahl der betroffenen Personen,
e. Kategorien und – soweit möglich – die ungefähre Anzahl der betroffenen personenbezogenen Datensätze,
f. die wahrscheinlichen Folgen der Datenschutzverletzung,
g. die bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Eindämmung und Behebung der Datenschutzverletzung sowie zur Minderung ihrer möglichen nachteiligen Auswirkungen,
h. Name und Kontaktdaten einer Ansprechperson für Rückfragen.

(3) Soweit einzelne Informationen zum Zeitpunkt der Erstmeldung noch nicht vorliegen, werden diese unverzüglich nachgereicht, sobald sie verfügbar sind.

(4) Der Auftragnehmer dokumentiert sämtliche Verletzungen des Schutzes personenbezogener Daten einschließlich ihrer Auswirkungen sowie der ergriffenen Abhilfemaßnahmen und stellt diese Dokumentation dem Auftraggeber auf berechtigtes Verlangen zur Verfügung, soweit gesetzlich zulässig.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner gesetzlichen Melde- und Benachrichtigungspflichten nach Art. 33 und Art. 34 DSGVO.

(6) Die Meldung einer Datenschutzverletzung durch den Auftragnehmer stellt kein Anerkenntnis einer Verantwortlichkeit oder Haftung dar.

§ 9 Kontrollrechte und Nachweise

(1) Der Auftragnehmer stellt dem Auftraggeber auf Verlangen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Verpflichtungen aus dieser Vereinbarung und aus Art. 28 DSGVO nachzuweisen.

(2) Zum Nachweis der Einhaltung kann der Auftragnehmer insbesondere geeignete Dokumentationen, Zertifizierungen, Prüfberichte unabhängiger Dritter, Selbstauskünfte oder vergleichbare Nachweise zur Verfügung stellen.

(3) Soweit die nach Absatz 2 bereitgestellten Nachweise zur Erfüllung gesetzlicher oder vertraglicher Prüfpflichten des Auftraggebers nicht ausreichen, ist der Auftraggeber berechtigt, nach vorheriger schriftlicher Ankündigung ein Audit beim Auftragnehmer durchzuführen oder durch einen zur Verschwiegenheit verpflichteten unabhängigen Dritten durchführen zu lassen.

(4) Audits sind mit einer angemessenen Frist, in der Regel mindestens 14 Kalendertage vorher anzukündigen und während der üblichen Geschäftszeiten durchzuführen. Sie dürfen den Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen. Dabei sind die berechtigten Geschäfts- und Betriebsgeheimnisse des Auftragnehmers sowie die Vertraulichkeit gegenüber anderen Kunden zu wahren.

(5) Der Auftragnehmer kann den Zugang zu Bereichen oder Informationen verweigern, soweit dadurch gesetzliche Geheimhaltungspflichten, Rechte Dritter, Sicherheitsanforderungen oder berechtigte Geschäftsgeheimnisse beeinträchtigt würden. In diesem Fall wird der Auftragnehmer dem Auftraggeber geeignete alternative Nachweise zur Verfügung stellen.

(6) Jede Partei trägt die ihr durch ein Audit entstehenden eigenen Kosten. Außergewöhnliche Aufwendungen des Auftragnehmers, die durch ein vom Auftraggeber veranlasstes Audit entstehen, können dem Auftraggeber nach vorheriger Abstimmung in angemessenem Umfang in Rechnung gestellt werden, sofern das Audit nicht aufgrund eines vom Auftragnehmer zu vertretenden Verstoßes erforderlich geworden ist.

§ 10 Löschung und Rückgabe personenbezogener Daten

(1) Nach Beendigung der vertraglich vereinbarten Leistungen verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers nur noch, soweit hierzu eine gesetzliche Verpflichtung besteht oder der Auftraggeber eine entsprechende Weisung erteilt hat.

(2) Der Auftragnehmer wird nach Wahl des Auftraggebers sämtliche personenbezogenen Daten sowie etwaige Datenträger und Unterlagen, die im Zusammenhang mit der Auftragsverarbeitung stehen,

a) an den Auftraggeber herausgeben oder
b) datenschutzgerecht löschen.

(3) Die Herausgabe oder Löschung erfolgt unverzüglich, spätestens jedoch innerhalb von **14 Kalendertagen** nach Zugang der entsprechenden Weisung des Auftraggebers, sofern gesetzliche Aufbewahrungspflichten oder sonstige gesetzliche Verpflichtungen nicht entgegenstehen.

(4) Soweit personenbezogene Daten aufgrund gesetzlicher Aufbewahrungspflichten weiterhin gespeichert werden müssen, werden diese für jede weitere Verarbeitung gesperrt und ausschließlich zur Erfüllung der gesetzlichen Verpflichtungen verarbeitet. Nach Ablauf der Aufbewahrungsfrist werden die Daten unverzüglich gelöscht.

(5) Der Auftragnehmer bestätigt dem Auftraggeber auf Verlangen die Durchführung der Löschung oder die vollständige Herausgabe der Daten in Textform.

(6) Sofern der Auftraggeber innerhalb von **30 Kalendertagen** nach Beendigung des Hauptvertrages keine Weisung zur Herausgabe oder Löschung erteilt, ist der Auftragnehmer berechtigt, die personenbezogenen Daten nach Ablauf gesetzlicher Aufbewahrungsfristen datenschutzgerecht zu löschen.

(7) Personenbezogene Daten, die sich ausschließlich auf Sicherungskopien (Backups) befinden, werden entsprechend den bestehenden Backup- und Löschkonzepten des Auftragnehmers gelöscht oder durch Überschreiben entfernt. Eine sofortige selektive Löschung einzelner Datensätze aus Backup-Medien ist nur geschuldet, soweit dies technisch möglich und wirtschaftlich zumutbar ist.

(8) Gesetzliche Herausgabe-, Aufbewahrungs- oder Nachweispflichten des Auftragnehmers bleiben unberührt.

§ 11 Haftung

(1) Die Haftung der Vertragsparteien richtet sich nach den gesetzlichen Vorschriften, insbesondere nach Art. 82 DSGVO sowie den einschlägigen Bestimmungen des Bürgerlichen Gesetzbuches (BGB).

(2) Der Auftragnehmer haftet nach Maßgabe der gesetzlichen Vorschriften für Schäden, die durch eine von ihm zu vertretende Verletzung dieser Vereinbarung oder der datenschutzrechtlichen Bestimmungen verursacht wurden.

(3) Der Auftraggeber haftet für Schäden, die auf einer rechtswidrigen oder fehlerhaften Weisung beruhen, soweit den Auftragnehmer kein Mitverschulden trifft.

(4) Soweit mehrere Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt sind und nach Art. 82 DSGVO für einen Schaden haften, gelten die gesetzlichen Regelungen über die gesamtschuldnerische Haftung sowie den internen Ausgleich.

(5) Die gesetzlichen Ansprüche betroffener Personen sowie die Haftungsregelungen der Datenschutz-Grundverordnung bleiben durch diese Vereinbarung unberührt.

§ 12 Vertragsdauer und Beendigung

(1) Diese Vereinbarung tritt mit Abschluss des Hauptvertrages in Kraft und gilt für dessen gesamte Laufzeit.

(2) Sie endet automatisch mit der Beendigung des Hauptvertrages, soweit keine gesetzlichen Aufbewahrungspflichten oder sonstigen gesetzlichen Verpflichtungen einer Beendigung entgegenstehen.

(3) Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Ein wichtiger Grund liegt insbesondere vor, wenn

a. eine Vertragspartei schwerwiegend oder wiederholt gegen die Bestimmungen dieser Vereinbarung oder gegen datenschutzrechtliche Vorschriften verstößt,

b. eine Vertragspartei ihren wesentlichen vertraglichen Verpflichtungen trotz angemessener Fristsetzung nicht nachkommt oder

c. die datenschutzkonforme Durchführung der Auftragsverarbeitung dauerhaft nicht mehr gewährleistet werden kann.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung einschließlich ihrer Anlagen bedürfen mindestens der Textform, sofern keine strengere gesetzliche Form vorgeschrieben ist.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Vertragsparteien verpflichten sich, die unwirksame oder undurchführbare Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen und rechtlichen Zweck der ursprünglichen Regelung möglichst nahekommt. Entsprechendes gilt für etwaige Vertragslücken.

(3) Es gilt das Recht der Bundesrepublik Deutschland unter Berücksichtigung der unmittelbar anwendbaren Vorschriften der Datenschutz-Grundverordnung (DSGVO).

(4) Sofern gesetzlich zulässig und beide Parteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliche Sondervermögen sind, ist Gerichtsstand der Sitz des Auftragnehmers.

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Pfändungen, Beschlagnahmen oder vergleichbare Maßnahmen Dritter, soweit personenbezogene Daten des Auftraggebers betroffen sein können und eine Mitteilung rechtlich zulässig ist.

(6) Bestandteil dieser Vereinbarung sind folgende Anlagen in ihrer jeweils gültigen Fassung:

- **Anlage 1** – Beschreibung der Verarbeitung personenbezogener Daten
- **Anlage 2** – Technische und organisatorische Maßnahmen (TOM)

- **Anlage 3** – Liste der Unterauftragnehmer
- **Informationsblatt**

Unterschrift

Auftraggeber	**Auftragnehmer**
Unternehmen / Einrichtung	CrayssnLabs GmbH
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Name	Für den Auftragnehmer
_____	_____
Funktion	
_____	
Unterschrift	Unterschrift
_____	_____

Datenschutzanfragen

CrayssnLabs GmbH

E-Mail: datenschutz@cl.team
Telefon: +49 361 23002016

Sofern gesetzlich ein Datenschutzbeauftragter bestellt ist, werden dessen Kontaktdaten dem Auftraggeber auf Anfrage oder über die Datenschutzhinweise des Auftragnehmers mitgeteilt.

Anlage 1

Beschreibung der Verarbeitung personenbezogener Daten

Stand: August 2026

1. Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erbringung der im Hauptvertrag vereinbarten IT-Dienstleistungen.

Je nach beauftragter Leistung umfasst dies insbesondere:

- Bereitstellung und Betrieb von Hosting- und Cloud-Diensten
- Betrieb und Administration von Servern und virtuellen Systemen
- Betrieb und Wartung von Websites, Webshops und Content-Management-Systemen
- Bereitstellung und Administration von E-Mail-Diensten
- Durchführung von Wartungs-, Support- und Administrationsleistungen
- Einrichtung, Migration und Pflege von IT-Systemen
- Datensicherung und Wiederherstellung (Backups)
- Fehleranalyse und Störungsbeseitigung
- Fernwartung und technischer Support
- Sicherheitsüberwachung der bereitgestellten Systeme
- Durchführung vereinbarter Entwicklungsleistungen

Die konkrete Verarbeitung richtet sich ausschließlich nach den im Hauptvertrag vereinbarten Leistungen.

2. Art der Verarbeitung

Je nach Leistungsumfang können insbesondere folgende Verarbeitungsvorgänge durchgeführt werden:

- Erheben
- Erfassen
- Organisieren
- Ordnen
- Speichern
- Anpassen
- Verändern
- Auslesen
- Abfragen
- Verwenden
- Offenlegen durch Übermittlung
- Bereitstellen

- Abgleichen
- Verknüpfen
- Einschränken
- Löschen
- Vernichten

3. Kategorien betroffener Personen

Je nach Nutzung der Leistungen können insbesondere folgende Personengruppen betroffen sein:

- Kunden des Auftraggebers
- Interessenten
- Besucher von Websites
- Nutzer von Online-Shops
- Mitarbeiter des Auftraggebers
- Bewerber
- Lieferanten
- Dienstleister
- Geschäftspartner
- Newsletter-Empfänger
- Benutzer von Kundenportalen
- Sonstige Personen, deren Daten der Auftraggeber im Rahmen seiner Geschäftstätigkeit verarbeitet

4. Kategorien personenbezogener Daten

Je nach Leistungsumfang können insbesondere folgende Daten verarbeitet werden:

Stammdaten • Name • Anschrift • Firma • Kundennummer	**Kontaktdaten** • Telefonnummer • E-Mail-Adresse • Faxnummer	**Vertragsdaten** • Vertragsinformationen • Bestellungen • Rechnungsdaten • Zahlungsinformationen
Kommunikationsdaten • E-Mails • Supportanfragen • Tickets • Chatverläufe	**Nutzungsdaten** • IP-Adressen • Logdaten • Zugriffszeiten • Browserinformationen • Geräteinformationen	**Inhaltsdaten** • Dateien • Dokumente • Bilder • Videos • Datenbankinhalte • Webseiteninhalte
Benutzerkonten • Benutzername • Passwort-Hash • Rollen • Berechtigungen		

Sonstige Daten
Sämtliche personenbezogenen Daten, die der Auftraggeber im Rahmen der Nutzung der vereinbarten Leistungen verarbeitet.

5. Kategorien besonderer personenbezogener Daten

Eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO erfolgt grundsätzlich nicht.

Soweit der Auftraggeber solche Daten im Rahmen der vereinbarten Leistungen verarbeitet, erfolgt die Verarbeitung ausschließlich auf Weisung des Auftraggebers und unter Anwendung geeigneter zusätzlicher technischer und organisatorischer Maßnahmen.

6. Empfänger personenbezogener Daten

Eine Übermittlung personenbezogener Daten erfolgt ausschließlich

- an den Auftraggeber,
- an vom Auftraggeber freigegebene Empfänger,
- an Unterauftragnehmer gemäß Anlage 3,
- soweit gesetzlich vorgeschrieben.

7. Drittlandübermittlungen

Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt grundsätzlich nicht.

Soweit im Einzelfall Drittlandübermittlungen erforderlich werden, erfolgen diese ausschließlich unter den Voraussetzungen der Art. 44 ff. DSGVO.

8. Dauer der Verarbeitung

Die Verarbeitung erfolgt ausschließlich für die Dauer des Hauptvertrages sowie darüber hinaus nur, soweit gesetzliche Aufbewahrungspflichten oder berechtigte gesetzliche Interessen dies erfordern.

Nach Beendigung des Vertragsverhältnisses richtet sich die Löschung oder Rückgabe personenbezogener Daten nach § 10 dieser Vereinbarung.

Anlage 2

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Stand: August 2026

1. Allgemeine Grundsätze

Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die Maßnahmen werden regelmäßig überprüft und bei Bedarf an den Stand der Technik sowie an geänderte Risiken angepasst.

2. Vertraulichkeit

2.1 Zutrittskontrolle

Der Zutritt zu Räumlichkeiten, in denen personenbezogene Daten verarbeitet oder technische Systeme betrieben werden, ist auf berechtigte Personen beschränkt.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- abschließbare Büroräume
- abschließbare Serverräume oder Serverschränke
- Schließsysteme
- Schlüsselverwaltung
- Besucherbegleitung
- keine unbeaufsichtigten Besucher in sicherheitsrelevanten Bereichen

2.2 Zugangskontrolle

Der Zugriff auf IT-Systeme erfolgt ausschließlich nach erfolgreicher Authentifizierung.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- individuelle Benutzerkonten
- sichere Kennwortrichtlinien
- rollenbasierte Benutzerverwaltung
- Multi-Faktor-Authentifizierung, soweit technisch verfügbar
- Sperrung oder Verzögerung weiterer Anmeldeversuche nach mehrfachen Fehlversuchen
- automatische Sitzungsbeendigung bei Inaktivität

2.3 Zugriffskontrolle

Berechtigte Personen erhalten ausschließlich Zugriff auf diejenigen Daten, die sie zur Erfüllung ihrer Aufgaben benötigen.

Hierzu werden insbesondere eingesetzt:

- Rollen- und Berechtigungskonzepte
- Need-to-know-Prinzip
- Rechteverwaltung
- Administratortrennung
- regelmäßige Überprüfung der Berechtigungen

2.4 Weitergabekontrolle

Personenbezogene Daten werden ausschließlich auf Weisung des Auftraggebers oder aufgrund gesetzlicher Verpflichtungen übermittelt.

Dabei kommen insbesondere folgende Maßnahmen zum Einsatz:

- verschlüsselte Datenübertragungen (TLS)
- VPN-Verbindungen für Administrationszugriffe
- verschlüsselte Fernwartungsverbindungen
- Zugriff nur durch autorisierte Personen

2.5 Trennungskontrolle

Personenbezogene Daten unterschiedlicher Auftraggeber werden logisch voneinander getrennt verarbeitet.

Dies erfolgt insbesondere durch:

- getrennte Datenbanken
- getrennte Dateisysteme
- getrennte Benutzerkonten
- getrennte Hosting-Umgebungen
- Mandantentrennung, soweit technisch vorgesehen

3. Integrität

3.1 Eingabekontrolle

Soweit technisch möglich und erforderlich werden Verarbeitungsvorgänge protokolliert.

Hierzu gehören beispielsweise:

- Administrationsprotokolle
- Anmeldeprotokolle
- Fehlerprotokolle

- Änderungsprotokolle
- Systemlogs

Die Protokolle werden ausschließlich zu Sicherheits-, Nachweis- und Fehleranalysezwecken verwendet.

3.2 Transportkontrolle

Personenbezogene Daten werden bei der Übertragung gegen unbefugte Kenntnisnahme geschützt.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- TLS-verschlüsselte Verbindungen
- SSH
- SFTP
- VPN
- verschlüsselte API-Kommunikation

4. Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle

Der Auftragnehmer trifft geeignete Maßnahmen, um die dauerhafte Verfügbarkeit der verarbeiteten personenbezogenen Daten sicherzustellen und Datenverluste möglichst zu vermeiden.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- regelmäßige Datensicherungen (Backups)
- redundante Speichersysteme, soweit eingesetzt
- unterbrechungsfreie Stromversorgung (USV), soweit vorhanden
- Überwachung der Server- und Netzwerkverfügbarkeit
- regelmäßige Prüfung der Systemauslastung
- Schutz vor Hardwareausfällen durch geeignete Ersatz- und Wiederherstellungsverfahren
- dokumentierte Wiederherstellungsprozesse

4.2 Backup- und Wiederherstellungskonzept

Zur Sicherstellung der Verfügbarkeit werden regelmäßig Sicherungskopien der verarbeiteten Daten erstellt, soweit dies Bestandteil der beauftragten Leistungen ist.

Dabei gelten insbesondere folgende Grundsätze:

- Durchführung regelmäßiger Datensicherungen
- Aufbewahrung der Sicherungen für einen definierten Zeitraum
- Schutz der Sicherungsmedien vor unbefugtem Zugriff
- regelmäßige Überprüfung der Wiederherstellbarkeit
- dokumentierte Wiederherstellungsverfahren

Die konkreten Sicherungsintervalle richten sich nach der jeweils vereinbarten Leistung und den technischen Gegebenheiten.

4.3 Notfallmanagement

Für sicherheitsrelevante Ereignisse bestehen organisatorische Verfahren zur schnellstmöglichen Wiederherstellung des ordnungsgemäßen Betriebs.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- dokumentierte Eskalationswege
- Störungsmanagement
- Wiederherstellungsverfahren
- Priorisierung kritischer Systeme
- Fehleranalyse nach sicherheitsrelevanten Vorfällen

4.4 Wiederherstellbarkeit

Der Auftragnehmer stellt durch geeignete organisatorische und technische Maßnahmen sicher, dass personenbezogene Daten und Systeme nach einem physischen oder technischen Zwischenfall innerhalb angemessener Zeit wiederhergestellt werden können.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- regelmäßige Tests von Wiederherstellungsverfahren
- dokumentierte Wiederanlaufprozesse
- Priorisierung kritischer Systeme
- regelmäßige Überprüfung der Backup-Integrität

4.5 Kontinuitätsplanung

Zur Aufrechterhaltung des Geschäftsbetriebs bestehen organisatorische Verfahren zur Bewältigung außergewöhnlicher Ereignisse.

Hierzu können insbesondere gehören:

- Vertretungsregelungen
- Wiederanlaufplanung
- Priorisierung kritischer Systeme
- Dokumentation wesentlicher Betriebsprozesse

5. Belastbarkeit und Systemsicherheit

5.1 Netzwerksicherheit

Die eingesetzten Systeme werden durch geeignete technische Maßnahmen gegen unbefugte Zugriffe geschützt.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- Firewall-Systeme
- Netzwerksegmentierung, soweit technisch umgesetzt
- abgesicherte Administrationszugänge
- regelmäßige Überprüfung offener Dienste
- Einschränkung unnötiger Netzwerkdienste

5.2 Systemhärtung

Server und Systeme werden nach anerkannten Sicherheitsgrundsätzen betrieben.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- regelmäßige Sicherheitsupdates
- zeitnahe Installation sicherheitsrelevanter Patches
- Deaktivierung nicht benötigter Dienste
- Einsatz aktueller Betriebssystemversionen
- regelmäßige Überprüfung der Systemkonfiguration

5.3 Schutz vor Schadsoftware

Zum Schutz vor Schadsoftware werden geeignete organisatorische und technische Maßnahmen eingesetzt.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- aktuelle Sicherheitsupdates
- Malware-Schutz, soweit technisch erforderlich
- eingeschränkte Benutzerrechte
- Überwachung sicherheitsrelevanter Ereignisse
- Prüfung installierter Software

5.4 Verschlüsselung

Personenbezogene Daten werden, soweit technisch möglich und unter Berücksichtigung der Art der Verarbeitung, durch geeignete kryptographische Verfahren geschützt.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- Transportverschlüsselung (TLS)
- Verschlüsselung administrativer Verbindungen
- Verschlüsselung mobiler Datenträger, soweit eingesetzt

- Verschlüsselung von Datensicherungen, soweit vorgesehen
- Sichere Verwaltung kryptographischer Schlüssel

6. Administrations- und Fernzugriffe

Administrationszugriffe erfolgen ausschließlich durch berechtigte Personen.

Hierbei werden insbesondere folgende Maßnahmen umgesetzt:

- personenbezogene Administratorzugänge
- verschlüsselte Fernzugriffe (z. B. VPN oder SSH)
- Protokollierung administrativer Zugriffe, soweit technisch möglich
- regelmäßige Überprüfung administrativer Berechtigungen
- Sperrung nicht mehr benötigter Benutzerkonten

7. Patch- und Änderungsmanagement

Zur Aufrechterhaltung der Systemsicherheit werden sicherheitsrelevante Aktualisierungen regelmäßig geprüft und zeitnah installiert.

Änderungen an produktiven Systemen erfolgen nach Möglichkeit kontrolliert und nachvollziehbar.
Soweit erforderlich werden Änderungen dokumentiert und vor der Umsetzung getestet.

8. Protokollierung und Monitoring

Zur Sicherstellung eines sicheren Betriebs werden sicherheitsrelevante Ereignisse überwacht.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- Systemprotokolle
- Authentifizierungsprotokolle
- Fehlerprotokolle
- Ressourcenüberwachung
- Sicherheitsereignisse

Die Protokolle dienen ausschließlich der Gewährleistung eines sicheren Betriebs, der Fehleranalyse sowie der Erfüllung gesetzlicher Nachweispflichten.

9. Verfahren zur regelmäßigen Überprüfung

Die technischen und organisatorischen Maßnahmen werden regelmäßig hinsichtlich ihrer Wirksamkeit überprüft und bei Bedarf angepasst.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- regelmäßige Sicherheitsüberprüfungen
- Bewertung neuer Risiken

- Überprüfung organisatorischer Prozesse
- Anpassung an gesetzliche Änderungen
- Anpassung an den Stand der Technik

10. Lösch- und Berechtigungskonzept

Personenbezogene Daten werden nach Ablauf gesetzlicher oder vertraglicher Aufbewahrungsfristen datenschutzgerecht gelöscht oder anonymisiert.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- geregelte Löschprozesse
- Löschung nicht mehr benötigter Benutzerkonten
- regelmäßige Überprüfung von Berechtigungen
- sichere Entsorgung von Datenträgern
- dokumentierte Löschprozesse, soweit erforderlich

10.1 Datenträgervernichtung

Nicht mehr benötigte Datenträger werden datenschutzgerecht gelöscht oder vernichtet.

Je nach Datenträgerart können geeignete Verfahren eingesetzt werden, um eine Wiederherstellung personenbezogener Daten auszuschließen.

11. Mobiles Arbeiten

Soweit personenbezogene Daten außerhalb der Geschäftsräume verarbeitet werden, gelten geeignete organisatorische und technische Schutzmaßnahmen.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- verschlüsselte Verbindungen
- gesicherte Endgeräte
- Bildschirmsperren
- aktuelle Betriebssysteme
- eingeschränkte Administratorrechte
- keine Nutzung ungesicherter öffentlicher WLANs ohne geeignete Schutzmaßnahmen

12. Unterauftragnehmer

Unterauftragnehmer werden vor ihrer Beauftragung hinsichtlich ihrer datenschutzrechtlichen und technischen Eignung geprüft.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- Abschluss einer AVV
- regelmäßige Überprüfung

- Dokumentation der eingesetzten Unterauftragnehmer
- Verpflichtung auf vergleichbare Sicherheitsmaßnahmen

13. Behandlung von Sicherheitsvorfällen

Für sicherheitsrelevante Ereignisse bestehen definierte Prozesse.

Je nach eingesetzter Infrastruktur können unter anderem folgende Maßnahmen umgesetzt werden:

- Erkennung
- Bewertung
- Dokumentation
- Eskalation
- Beseitigung
- Nachbereitung

14. Datenschutz durch Technikgestaltung

Neue Systeme und Verfahren werden unter Berücksichtigung datenschutzrechtlicher Anforderungen geplant und umgesetzt.

Soweit technisch und organisatorisch möglich werden datenschutzfreundliche Voreinstellungen berücksichtigt.

15. Sensibilisierung

Mitarbeiter werden regelmäßig hinsichtlich

- Datenschutz
- Informationssicherheit
- IT-Sicherheit
- Vertraulichkeit

sensibilisiert.

15.1 Verantwortlichkeiten

Datenschutz- und Informationssicherheitsaufgaben werden innerhalb des Unternehmens organisatorisch geregelt.

Zugriffsberechtigungen und Verantwortlichkeiten werden dokumentiert und regelmäßig überprüft.

16. Dokumentation

Die wesentlichen Sicherheitsmaßnahmen sowie sicherheitsrelevante organisatorische Prozesse werden dokumentiert und regelmäßig aktualisiert.

Anlage 3
Eingesetzte Unterauftragnehmer

Stand: August 2026

Allgemeines

Der Auftragnehmer setzt zur Erbringung der vertraglich vereinbarten Leistungen gegebenenfalls Unterauftragnehmer gemäß § 6 der Auftragsverarbeitungsvereinbarung ein.

Sämtliche Unterauftragnehmer werden vor ihrer Beauftragung hinsichtlich ihrer datenschutzrechtlichen und technischen Eignung geprüft und – soweit erforderlich – vertraglich gemäß Art. 28 DSGVO verpflichtet.

Änderungen der eingesetzten Unterauftragnehmer erfolgen nach Maßgabe von § 6 der Auftragsverarbeitungsvereinbarung.

Aktuell eingesetzte Unterauftragnehmer

Dienstleister 1:
Name des Dienstleisters: dogado GmbH
Anschrift: Antonio-Segni-Straße 11, 44263 Dortmund
Art der Dienstleistung: Hosting-Umgebung, Rechenzentrum, Cloud-Speicher
Bestellter Datenschutzbeauftragter (DSB): Alfahosting GmbH
Kontaktdaten des DSB: datenschutz@dogado.de

Dienstleister 2:
Name des Dienstleisters: InterNetX GmbH
Anschrift: Johanna-Dachs-Str. 55, 93055 Regensburg
Art der Dienstleistung: Domain- & DNS-Management
Bestellter Datenschutzbeauftragter (DSB): InterNetX GmbH
Kontaktdaten des DSB: datenschutz@internetx.com

Dienstleister 3:
Name des Dienstleisters: N-able Technologies Ltd.
Anschrift: Suites 11 &12, The Vision Building, 20 Greenmarket,
Dundee, DD1 4QB, UK
Art der Dienstleistung: Spam-Gateway
Bestellter Datenschutzbeauftragter (DSB): Jason Bliss
Kontaktdaten des DSB: privacy@n-able.com

Dienstleister 4:
Name des Dienstleisters: OpenAI OpCo, LLC
Anschrift: 1455 3rd Street, San Francisco, CA 94158

Art der Dienstleistung: API-Zugriff für Sprachmodelle sowie Text-to-Speech- und Speech-to-Text-Dienste
Bestellter Datenschutzbeauftragter (DSB): Emma Redmond
Kontaktdaten des DSB: privacy@openai.com

Dienstleister 5:
Name des Dienstleisters: Keyweb AG
Anschrift: Neuwerkstraße 45/46, 99084 Erfurt
Art der Dienstleistung: Hosting-Umgebung, Rechenzentrum, Cloud-Speicher
Bestellter Datenschutzbeauftragter (DSB): Keyweb AG
Kontaktdaten des DSB: datenschutz@keyweb.de

Hinweise zu Drittlandübermittlungen

Soweit Unterauftragnehmer personenbezogene Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten, erfolgt dies ausschließlich unter Einhaltung der Art. 44 ff. DSGVO.

Hierzu können insbesondere folgende geeignete Garantien eingesetzt werden:

- Angemessenheitsbeschluss der Europäischen Kommission,
- Standardvertragsklauseln (SCC),
- sonstige gesetzlich zulässige Übermittlungsmechanismen.

Verpflichtungen der Unterauftragnehmer

Der Auftragnehmer stellt sicher, dass Unterauftragnehmer mindestens zu folgenden Pflichten verpflichtet werden:

- Verarbeitung ausschließlich auf dokumentierte Weisung,
- Vertraulichkeit,
- geeignete technische und organisatorische Maßnahmen,
- Unterstützung bei Betroffenenrechten,
- Unterstützung bei Datenschutzverletzungen,
- Löschung oder Rückgabe personenbezogener Daten nach Vertragsende,
- Duldung von Kontrollen gemäß Art. 28 DSGVO.

Informationsblatt
Ansprechpartner und Kommunikationswege

Stand: August 2026

Diese Anlage enthält die Ansprechpartner und Kommunikationswege für datenschutz- und sicherheitsrelevante Angelegenheiten im Zusammenhang mit der Auftragsverarbeitungsvereinbarung.

1. Auftragnehmer

CrayssnLabs GmbH
Kartäuserstraße 21d
99084 Erfurt

2. Datenschutzanfragen

E-Mail: datenschutz@cl.team
Telefon: +49 361 23002016

3. Meldung von Datenschutzverletzungen und Sicherheitsvorfällen

E-Mail: info@cl.team
Telefon: +49 361 23002016

4. Ansprechpartner

Die Bearbeitung erfolgt durch die jeweils zuständige Fachstelle der CrayssnLabs GmbH.

5. Reaktionszeiten

Der Auftragnehmer bearbeitet datenschutz- und sicherheitsrelevante Meldungen mit angemessener Priorität. Dabei gelten insbesondere folgende Grundsätze:

- Datenschutzverletzungen: unverzügliche Bearbeitung nach Bekanntwerden
- Sicherheitsvorfälle: unverzügliche Bearbeitung nach Bekanntwerden
- Betroffenenanfragen: Bearbeitung innerhalb der gesetzlichen Fristen

Dokumentenhistorie

Version	Datum	Änderung
1.0	August 2026	Erstfassung