Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO

zwischen

Firmenname:
Adresse:
PLZ, Stadt:

– im Folgenden: Auftraggeber –

und der

Twinwin GmbH
c/o Bauermeister
Boddinstr. 24a
12053 Berlin

– im Folgenden: Auftragnehmer –

Der Auftraggeber (für die Verarbeitung verantwortlich) und der Auftragnehmer schließen den folgenden Vertrag zur Auftragsverarbeitung gemäß Art. 28 der europäischen Datenschutz-Grundverordnung (DSGVO). Auf Grundlage des zwischen den Parteien bestehenden Vertragsverhältnisses (Hauptvertrag) verarbeitet der Auftragnehmer personenbezogene Daten für den Auftraggeber. Die sich daraus ergebenden datenschutzrechtlichen Rechte und Verpflichtungen der Parteien werden durch diesen Auftragsverarbeitungsvertrag konkretisiert.

§ 1 Gegenstand und Dauer der Verarbeitung

1. Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten" genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung. Der Gegenstand und die Dauer des Vertrages richten sich nach dem Hauptvertrag.

2. Der Auftraggeber kann diesen Vertrag sowie den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieser Vereinbarung vorliegt und der Auftragnehmer diesen Verstoß trotz schriftlicher Abmahnung und Setzung einer angemessenen Abhilfefrist von mindestens 14 Werktagen nicht behoben hat. Ein schwerwiegender Verstoß liegt insbesondere dann vor, wenn der Auftragnehmer die Daten des Auftraggebers für andere als die nach dieser Vereinbarung bestimmten Zwecke verwendet oder gegen eine wesentliche Pflicht aus dieser Vereinbarung verstößt. Das Recht zur fristlosen Kündigung ohne vorherige Abhilfefrist bleibt unberührt, wenn der Verstoß seiner Natur nach nicht behebbar ist.

3. Auch bei Nichtvorliegen der zuvor genannten Voraussetzungen ist der Auftraggeber berechtigt, diese Vereinbarung und den Hauptvertrag fristlos zu kündigen, wenn der Auftragnehmer wiederholt gegen diese Vereinbarung verstößt. Ein vorheriger schriftlicher Hinweis oder ein Hinweis in Textform des Auftraggebers ist hierfür Voraussetzung.

4. Der Auftragnehmer ist berechtigt, diesen Vertrag sowie den Hauptvertrag fristlos zu kündigen, wenn der Auftraggeber trotz schriftlicher Aufforderung wiederholt Weisungen erteilt, die gegen datenschutzrechtliche Vorschriften verstoßen, oder seinen Mitwirkungspflichten aus diesem Vertrag wiederholt nicht nachkommt.

§ 2 Umfang, Art und Zweck der Verarbeitung

1. Umfang, Art und Zweck der Verarbeitung personenbezogener Daten ergeben sich aus dem zwischen den Parteien geschlossenen Dienstleistungsvertrag sowie aus der Anlage B zu diesem Vertrag.

2. Die Anlage B enthält eine Aufschlüsselung der Verarbeitungstätigkeiten, der jeweils verarbeiteten Datenkategorien, der betroffenen Personengruppen sowie der jeweiligen Zwecke. Sie ist Bestandteil dieses Vertrages und wird bei wesentlichen Änderungen des Leistungsumfangs entsprechend aktualisiert.

3. Der Auftragnehmer ist berechtigt, die Anlage B einseitig zu aktualisieren, soweit dies zur Abbildung von Änderungen des Leistungsumfangs erforderlich ist, die sich aus dem Hauptvertrag, einschließlich der jeweils gültigen Leistungsbeschreibung und der AGB, ergeben. Dies umfasst insbesondere die Aufnahme neuer Module, die Anpassung von Datenkategorien und betroffenen Personengruppen sowie die Aktualisierung von Rechtsgrundlagen. Voraussetzung ist, dass der Auftraggeber über die Aktualisierung in Textform informiert wird. Der Verarbeitungsumfang darf nicht über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen. Für Aktualisierungen, die sich nicht aus dem Hauptvertrag ableiten lassen, ist eine ausdrückliche Vereinbarung der Parteien erforderlich.

§ 3 Art der personenbezogenen Daten

Der Auftragnehmer erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt dem Auftragnehmer folgende personenbezogene Daten zu erheben:

- Personenstammdaten
- Kontaktdaten
- Vertrags- und Abrechnungsdaten
- Nutzungs- und Protokolldaten

- Beschäftigtendaten
- Ggf. besondere Datenkategorien im Sinne des Art. 9 DSGVO (vgl. Anlage B)

§ 4 Kreis der betroffenen Personen

Bei den betroffenen Personen der oben aufgelisteten Daten handelt es sich um:

- Mitarbeiter des Auftraggebers (Plattformnutzer)
- Beschäftigte des Auftraggebers (in der Regel keine Plattformnutzer)
- Freie Mitarbeiter, Praktikanten und Auszubildende des Auftraggebers
- Ansprechpartner und Vertretungsberechtigte des Auftraggebers
- Eingeladene, noch nicht registrierte Personen
- Sonstige Personen, deren Daten der Auftraggeber im Rahmen der Plattformnutzung eingibt

§ 5 Rechte und Pflichten des Auftraggebers; Kontrollrechte

1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und somit Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

2. Der Auftraggeber ist dafür verantwortlich, die Informationspflichten gegenüber den betroffenen Personen gemäß Art. 13 und Art. 14 DSGVO vollständig zu erfüllen. Dies umfasst insbesondere die Information über die Auftragsverarbeitung durch den Auftragnehmer, die Kategorien der verarbeiteten Daten sowie die Rechte der betroffenen Personen. Der Auftragnehmer unterstützt den Auftraggeber auf Anfrage bei der Erfüllung dieser Pflichten, insbesondere durch Bereitstellung der erforderlichen Informationen über die beim Auftragnehmer stattfindende Verarbeitung.

3. Der Auftraggeber erteilt dem Auftragnehmer Weisungen über die Art und den Umfang der Verarbeitung der personenbezogenen Daten. Weisungen sind in Textform zu erteilen (z. B. per E-Mail oder über das Ticketsystem der Plattform). Mündlich erteilte Weisungen sind unverzüglich in Textform zu bestätigen. Der Auftragnehmer ist berechtigt, die Ausführung mündlicher, nicht in Textform bestätigter Weisungen bis zur Bestätigung auszusetzen.

4. Der Auftraggeber ist berechtigt, sich nach rechtzeitiger vorheriger Anmeldung mit einer Frist von mindestens 14 Werktagen zu den üblichen Geschäftszeiten von der Einhaltung der bei dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen, sofern dieser zur Vertraulichkeit verpflichtet ist. Das Kontrollrecht ist auf eine Prüfung pro Kalenderjahr beschränkt, sofern kein begründeter Verdacht eines Datenschutzverstoßes vorliegt. Der Auftraggeber hat sicherzustellen, dass die Kontrolle den Betriebsablauf des

Auftragnehmers so gering wie möglich beeinträchtigt und Betriebs- und Geschäftsgeheimnisse des Auftragnehmers gewahrt bleiben. Die Kosten einer Vor-Ort-Kontrolle trägt der Auftraggeber. Soweit der Auftragnehmer den Nachweis der Einhaltung seiner Pflichten durch geeignete Zertifizierungen oder aktuelle Auditberichte erbringt (vgl. Abs. 6), kann dies an die Stelle einer Vor-Ort-Kontrolle treten.

5. Der Auftragnehmer hat eventuelle Kontrollmaßnahmen der Datenschutzaufsichtsbehörde gem. Art. 58 DSGVO und § 40 BDSG zu dulden. Er wird den Auftraggeber unverzüglich nach Ankündigung oder Kenntniserlangung über die Durchführung der Kontrollmaßnahme sowie bei anderweitigen Anfragen, Ermittlungen oder Erkundigungen der Datenschutzaufsichtsbehörde, insbesondere auch, wenn diese im Rahmen einer vorherigen Konsultation gem. Art. 36 DSGVO erfolgen, informieren, soweit die Maßnahmen oder Anfragen Datenverarbeitungen betreffen können, die der Auftragnehmer für den Auftraggeber erbringt.

6. Auf Verlangen des Auftraggebers weist der Auftragnehmer die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen auf geeignete Weise nach. Die Form des Nachweises bestimmt der Auftragnehmer; sie umfasst insbesondere Selbstauskünfte, interne Auditberichte oder, soweit vorhanden, Zertifizierungen oder externe Testate. Die Kontrollrechte des Auftraggebers bleiben hiervon unberührt.

§ 6 Pflichten des Auftragnehmers

1. Der Auftragnehmer ist verpflichtet, personenbezogene Daten ausschließlich weisungsgemäß und nach den Vorgaben dieses Vertrages zu verarbeiten.

2. Bei der Gewährung der Rechte der Betroffenen gemäß Art. 15 ff. DSGVO (Berichtigung, Einschränkung der Verarbeitung, Löschung, Benachrichtigung und Auskunftserteilung) wird der Auftragnehmer den Auftraggeber auf Anforderung im Rahmen seiner Möglichkeiten unterstützen. Die Prüfung der Berechtigung des jeweiligen Betroffenenantrags obliegt dem Auftraggeber. Der Auftragnehmer wird hierfür geeignete technische und organisatorische Maßnahmen treffen. Der Auftragnehmer hat auf Weisung die personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Soweit die Unterstützung des Auftragnehmers bei der Erfüllung datenschutzrechtlicher Pflichten des Auftraggebers – einschließlich der Betroffenenrechte, Meldepflichten und Informationspflichten – über die standardmäßig in der Plattform bereitgestellten Funktionen hinausgeht, ist der Auftragnehmer berechtigt, den hierfür entstehenden angemessenen Aufwand gegenüber dem Auftraggeber geltend zu machen.

3. Sollten die im Auftrag des Auftraggebers erhobenen Daten Gegenstand eines Verlangens auf Datenportabilität gemäß Art. 20 DSGVO sein, wird der Auftragnehmer dem Auftraggeber den betreffenden Datensatz in der Regel innerhalb von 30 Tagen

auf Anforderung in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen. Soweit die Bereitstellung über die standardmäßig in der Plattform verfügbaren Exportfunktionen hinausgeht, ist der Auftragnehmer berechtigt, den hierfür entstehenden angemessenen Aufwand gegenüber dem Auftraggeber geltend zu machen.

4. Sofern sich eine betroffene Person unmittelbar an den Auftragnehmer mit der Wahrnehmung ihrer Betroffenenrechte wendet, hat dieser dieses Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn er der Meinung ist, dass eine erteilte Weisung gegen gesetzliche Vorschriften verstößt. Die Durchführung der entsprechenden Weisung kann er solange aussetzen, bis sie durch den Auftraggeber bestätigt oder abgeändert wird. Der Auftragnehmer haftet nicht für Schäden, die aus der Befolgung einer rechtswidrigen Weisung des Auftraggebers entstehen.

6. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Kenntnis davon erlangt, dass bei der Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages gegen datenschutzrechtliche Vorschriften oder gegen die in diesem Vertrag getroffenen Festlegungen verstoßen wurde. Dies gilt insbesondere bei Verstößen gegen die Pflichten aus diesem Vertrag durch Mitarbeiter oder Beauftragte des Auftragnehmers. Für Verletzungen des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO gilt ergänzend § 6a.

7. Nach Beendigung des Hauptvertrages wird der Auftragnehmer auf Weisung des Auftraggebers sämtliche personenbezogenen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, in einem vom Auftragnehmer unterstützten, maschinenlesbaren Format aushändigen oder datenschutzkonform löschen. Der Auftraggeber teilt seine Weisung innerhalb von 60 Tagen nach Vertragsende mit; nach Ablauf dieser Frist ist der Auftragnehmer zur Löschung berechtigt. Die Löschung wird innerhalb von 90 Tagen nach Weisungserteilung bzw. nach Ablauf der Mitteilungsfrist durchgeführt. Daten in automatisierten Backup-Systemen werden im Rahmen der regulären Backup-Rotation gelöscht, spätestens jedoch innerhalb von 180 Tagen.

8. Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

§ 6a Meldepflichten bei Datenschutzverletzungen

1. Der Auftragnehmer wird den Auftraggeber unverzüglich nach Kenntniserlangung über jede Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO informieren, die im Zusammenhang mit der Auftragsverarbeitung steht. Die Meldung erfolgt, sobald dem Auftragnehmer hinreichend gesicherte Informationen vorliegen, in der Regel innerhalb von 48 Stunden nach Kenntniserlangung, um dem Auftraggeber die Einhaltung seiner Meldepflicht gemäß Art. 33 DSGVO zu ermöglichen.

2. Die Meldung muss mindestens folgende Informationen enthalten, soweit diese zum Zeitpunkt der Meldung vorliegen:
   - Art der Datenschutzverletzung einschließlich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze
   - Name und Kontaktdaten des Ansprechpartners beim Auftragnehmer
   - Beschreibung der wahrscheinlichen Folgen der Verletzung
   - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung der möglichen nachteiligen Auswirkungen

3. Soweit die Informationen nicht gleichzeitig zur Verfügung gestellt werden können, stellt der Auftragnehmer diese unverzüglich schrittweise bereit.

4. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) und gegenüber den betroffenen Personen (Art. 34 DSGVO). Die Dokumentation von Datenschutzverletzungen einschließlich der mit ihnen zusammenhängenden Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen erfolgt durch den Auftragnehmer und wird dem Auftraggeber auf Anforderung zur Verfügung gestellt.

§ 7 Leistungsort

1. Die Verarbeitung und Nutzung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Soweit im Rahmen der genehmigten Unterauftragsverhältnisse (§ 8) eine Verarbeitung in Drittländern erfolgt, gelten die Regelungen in Abs. 2. Im Übrigen bedarf jede Verlagerung in ein Drittland der vorherigen Zustimmung durch den Auftraggeber und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Sofern die Verarbeitung personenbezogener Daten außerhalb der EU/des EWR erfolgt, garantiert der Auftragnehmer, dass die nach den jeweils geltenden Datenschutzvorschriften anwendbaren Voraussetzungen erfüllt sind. Dies umfasst insbesondere das Vorliegen eines Angemessenheitsbeschlusses der EU-Kommission

(Art. 45 DSGVO), die Vereinbarung von EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO) oder das Vorhandensein sonstiger geeigneter Garantien gemäß Art. 46 DSGVO.

§ 8 Unterauftragsverhältnisse

1. Der Auftraggeber erteilt hiermit seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO zur Hinzuziehung weiterer Auftragsverarbeiter durch den Auftragnehmer. Vor Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters informiert der Auftragnehmer den Auftraggeber.
2. Der Auftraggeber kann der Änderung innerhalb von 14 Werktagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Dieses ist innerhalb von vier Wochen nach endgültigem Scheitern der Einigungsverhandlungen in Textform auszuüben.
3. Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragnehmer haftet für die sorgfältige Auswahl und vertragliche Verpflichtung der weiteren Auftragsverarbeiter.
4. Der Auftragnehmer hat die Einhaltung der Pflichten des weiteren Auftragsverarbeiters regelmäßig zu überprüfen. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der weitere Auftragsverarbeiter die zugesicherten und erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.
5. Der Auftragnehmer arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Auftraggeber einverstanden erklärt:

Name des Unter-auftragsverarbeiters	**Beschreibung der Leistungen**
Hetzner Online GmbH	Serverinfrastruktur, Dedicated Server, Cloud-Hosting
Okta, Inc.	Authentifizierung und Login (Auth0)
DigitalOcean, LLC	Serverinfrastruktur, Cloud-Hosting, Medienspeicher (Spaces)

Google Ireland Ltd.	Cloud-Dienste, E-Mail, Kalender, Dokumentenverwaltung (Google for Business)
HubSpot Ireland Ltd.	CRM-System
MailerSend Ltd.	E-Mail-Versanddienst (Einladungen, Benachrichtigungen, Verifizierung etc.)
BunnyWay d.o.o.	Video- und Static-File-Hosting (CDN)
Cloudflare, Inc.	Caching, DNS, DDoS-Schutz
Celonis SE	Automation, Webhooks, Middleware (Make.com)

§ 9 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung gem. Art. 32 i.V.m. Art. 5 Abs. 1 DSGVO einzuhalten. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen, mit denen eine angemessene Pseudonymisierung und Verschlüsselung gewährleistet werden kann sowie Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten.
2. Die von dem Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind ausführlich in der Anlage A zu diesem Vertrag dargestellt und sind Vertragsbestandteil.
3. Der Auftragnehmer überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 lit. d DSGVO regelmäßig. Die Ergebnisse der Überprüfung sind zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen. Ergibt die Überprüfung Anpassungsbedarf, setzt der Auftragnehmer die erforderlichen Maßnahmen unverzüglich um.
4. Der Auftragnehmer wird das Sicherheitsniveau der technischen und organisatorischen Maßnahmen während der Vertragslaufzeit nicht unterschreiten. Anpassungen, die das Sicherheitsniveau wesentlich verändern, sind dem Auftraggeber unverzüglich mitzuteilen.
5. Der Auftragnehmer ist berechtigt, die in Anlage A beschriebenen technischen und organisatorischen Maßnahmen einseitig zu aktualisieren, sofern die folgenden Voraussetzungen kumulativ erfüllt sind:

a. Die Aktualisierung dient der Anpassung an den Stand der Technik, der Umsetzung gesetzlicher oder behördlicher Anforderungen, der Behebung von Sicherheitslücken, der Verbesserung des Schutzniveaus oder der Reduzierung von Drittlandtransferrisiken (z.B. Verlagerung von Datenverarbeitungen in den EU/EWR-Raum).

b. Das Sicherheitsniveau der technischen und organisatorischen Maßnahmen wird durch die Aktualisierung insgesamt nicht unterschritten.

6. Für die Durchführung einer Aktualisierung nach Abs. 5 gilt folgendes Verfahren:

   a. Der Auftragnehmer informiert den Auftraggeber mindestens 14 Werktage vor dem geplanten Wirksamwerden der Aktualisierung in Textform über die beabsichtigten Änderungen. Die Mitteilung enthält eine Beschreibung der geänderten Maßnahmen.

   b. Der Auftraggeber kann der Aktualisierung innerhalb von 14 Werktagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Aktualisierung als genehmigt. Im Falle eines Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung.

   c. Bei Maßnahmen zur Behebung akuter Sicherheitslücken, zur Erfüllung behördlicher Anordnungen oder infolge des Wegfalls oder der wesentlichen Einschränkung einer Transfergrundlage für Drittlandtransfers (insbesondere Aufhebung oder Aussetzung eines Angemessenheitsbeschlusses gem. Art. 45 DSGVO, Unwirksamkeit vereinbarter Standardvertragsklauseln oder vergleichbare Ereignisse) kann der Auftragnehmer die Aktualisierung sofort umsetzen und den Auftraggeber unverzüglich nachträglich informieren. Das Widerspruchsrecht des Auftraggebers bleibt in diesem Fall unberührt; ein Widerspruch entfaltet jedoch erst ab Zugang Wirkung.

   d. Der Auftragnehmer hält die jeweils aktuelle Fassung der Anlage A vor und stellt diese dem Auftraggeber auf Anforderung zur Verfügung.

§ 10 Haftung

1. Der Auftragnehmer haftet gegenüber dem Auftraggeber gemäß der gesetzlichen Regelungen für Schäden durch schuldhafte Verstöße gegen diesen Vertrag sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen, vorbehaltlich der Beschränkungen in Abs. 4.

2. Für den Ersatz von Schäden, die ein Betroffener aufgrund einer nach der DSGVO oder dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder

unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses geltend macht, sind der Auftraggeber bzw. der Auftragnehmer gem. Art. 82 DSGVO gegenüber dem Betroffenen verantwortlich. Der Auftragnehmer stellt den Auftraggeber im Innenverhältnis von allen Schadensersatzansprüchen frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus diesem Vertrag durch den Auftragnehmer gegen den Auftraggeber geltend gemacht werden. Die Freistellungspflicht besteht im Rahmen der Haftungsbegrenzungen dieses Vertrages gemäß Abs. 4.

3. Der Auftraggeber stellt den Auftragnehmer im Innenverhältnis von allen Schadensersatzansprüchen frei, die Dritte oder betroffene Personen gegen den Auftragnehmer geltend machen, soweit diese auf einer rechtswidrigen oder fehlerhaften Weisung des Auftraggebers, auf einer Verletzung der Pflichten des Auftraggebers aus diesem Vertrag oder auf der Verarbeitung rechtswidrig bereitgestellter Daten beruhen.

4. Die Haftung des Auftragnehmers für leichte Fahrlässigkeit ist auf den vorhersehbaren, vertragstypischen Schaden begrenzt, höchstens jedoch auf die vom Auftraggeber in den zwölf Monaten vor dem Schadensereignis gezahlte Vergütung. Dies gilt nicht für Schäden aus der Verletzung von Leben, Körper oder Gesundheit sowie bei Vorsatz oder grober Fahrlässigkeit.

§ 11 Schlussbestimmungen

1. Im Falle von Widersprüchen zwischen den datenschutzspezifischen Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor. Im Übrigen gelten die Regelungen des Hauptvertrages. Haftungsbeschränkungen aus dem Hauptvertrag gelten auch für Ansprüche aus diesem Auftragsverarbeitungsvertrag, soweit gesetzlich zulässig.

2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform und der ausdrücklichen Angabe, dass damit die Bestimmungen des geltenden AVV geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Sollte eine Bestimmung dieser Vereinbarung unwirksam oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die unwirksame oder nicht durchsetzbare Bestimmung ist durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, welche dem Zweck der ersetzenden Bestimmung am nächsten kommt.

4. Soweit dieser Vertrag einschließlich seiner Anlagen auf gesetzliche Vorschriften Bezug nimmt, sind diese in ihrer jeweils geltenden Fassung maßgeblich. Treten an die Stelle der in Bezug genommenen Vorschriften Nachfolgeregelungen, so treten diese an deren Stelle. Dies gilt insbesondere für Verweise auf Vorschriften des BDSG, der DSGVO sowie des sonstigen anwendbaren Datenschutzrechts.

5. Dieser Auftragsverarbeitungsvertrag ersetzt mit seinem Abschluss sämtliche zwischen den Parteien zuvor geschlossenen Vereinbarungen zur Auftragsverarbeitung, gleich welcher Form oder Bezeichnung. Etwaige Rechte und Pflichten aus dem bisherigen Auftragsverarbeitungsverhältnis, die zum Zeitpunkt des Abschlusses dieses Vertrages bereits entstanden sind, bleiben unberührt.

6. Soweit die Daten des Auftraggebers oder der Zugriff darauf seitens des Auftragnehmers durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige, nicht von den vorstehenden Regelungen erfasste Ereignisse gefährdet werden sollten, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu benachrichtigen.

7. Diese Vereinbarung unterliegt deutschem Recht.

ppa. Karol M. Czuba
Twinwin GmbH

Stand: 22. April 2026

Anlage A: Technische und organisatorische Maßnahmen

Der Auftragnehmer versichert, die folgenden technischen und organisatorische Maßnahmen getroffen zu haben:

1. Maßnahmen zur Sicherung der Vertraulichkeit

a) Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Beschreibung des Zutrittskontrollsystems:

- kontrollierte Schlüsselvergabe
- Türsicherung
- Kontrollsystem für Besucher

b) Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Authentifizierung über standardisierte Protokolle wie OpenID Connect bzw. OAuth2 sowie passwortbasierte Anmeldung mit serverseitig erzwungenen Passwortrichtlinien (Mindestlänge, Zeichenkomplexität, Ausschluss gängiger Passwörter)
- Automatische Session-Invalidierung nach definiertem Inaktivitäts-Timeout; verkürzte Session-Laufzeit für besonders sensible Nutzer-Rollen
- Schutz von Authentifizierungsendpunkten gegen automatisierte Angriffe (Rate Limiting)
- Sichere Übertragung durch HTTPS-Erzwingung, HSTS, Secure-Cookie-Flag und CSRF-Schutz in Produktivumgebungen
- Einrichtung eines Benutzerstammsatzes pro User
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Verschlüsselung von Datenträgern
- Einrichten von regelmäßigen aktualisierten Antiviren- und Spywarefiltern

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- Rollenbasiertes Berechtigungskonzept mit differenzierten Zugriffsebenen; Berechtigungen der Rollen werden individuell konfiguriert
- Zugriff auf Funktionen und Datenbereiche wird abhängig von Rolle und Berechtigungsstufe auf Anwendungsebene gesteuert

Im Hinblick auf Mitarbeiter des Auftragnehmers:

- Zugriffsberechtigungen werden auf Basis der jeweiligen Tätigkeit und des Grundsatzes der minimalen Rechtevergabe vergeben, dokumentiert und bei Änderung der Tätigkeit oder des Beschäftigungsverhältnisses angepasst
- Mitarbeiter mit Zugriff auf personenbezogene Daten werden vor Aufnahme ihrer Tätigkeit über datenschutzkonforme Verarbeitung, geltende Zugriffsbeschränkungen und die Grenzen des zulässigen Umgangs mit diesen Daten unterwiesen

d) Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Mandantenbezogene Zugriffstrennung ist auf Anwendungsebene systemisch verankert; jeder Datenzugriff wird anhand der Auftraggeberzuordnung geprüft
- Die Wirksamkeit der Isolation wird durch automatisierte Sicherheitstests kontinuierlich verifiziert
- Verschlüsselte Speicherung von personenbezogenen Daten

e) Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei

durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung des Pseudonymisierungsverfahrens:

- Hashwertverfahren nach aktuellem Stand der Technik

2. Maßnahmen zur Sicherung der Integrität

a) Weitergabekontrolle

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

Beschreibung der Weitergabekontrolle:

- Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen
- Transportprozesse mit individueller Verantwortlichkeit
- sicherer Transportbehälter für Datenträger

b) Eingabekontrolle

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

Beschreibung des Eingabekontrollvorgangs:

- Erstellungs-, Änderungs- und Löschvorgänge auf Modellen mit personenbezogenen Daten werden vollständig protokolliert
- Jeder Protokolleintrag erfasst Zeitpunkt, ausführenden Nutzer, betroffenes Objekt und Art der Aktion
- Protokolleinträge sind auf Anwendungsebene vor nachträglicher Veränderung geschützt
- Protokolldaten werden für einen dem Schutzbedarf entsprechenden Zeitraum aufbewahrt und anschließend automatisiert gelöscht

3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

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

Beschreibung des Verfügbarkeitskontrollsystems:

- Regelmäßige automatisierte Datensicherung mit definierter Aufbewahrungsdauer
- Geografisch getrennte Aufbewahrung der Backup-Kopien an voneinander unabhängigen Standorten
- Dokumentiertes Backup-Konzept mit festgelegten Sicherungsintervallen

b) Rasche Wiederherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen:

- Datensicherungsverfahren mit definierten Wiederherstellungszielen
- Regelmäßige Tests der Datenwiederherstellung zur Überprüfung der tatsächlichen Wiederherstellungsfähigkeit

c) Patch- und Schwachstellenmanagement

Maßnahmen, die sicherstellen, dass bekannte Sicherheitslücken in eingesetzter Software und Infrastruktur zeitnah identifiziert und behoben werden.

Beschreibung der Maßnahmen:

- Automatisierte Schwachstellenprüfung von Softwareabhängigkeiten als Bestandteil des Deployment-Prozesses
- Regelmäßige Überprüfung und Aktualisierung eingesetzter Komponenten anhand einschlägiger Schwachstellenquellen
- Regelmäßige Sicherheitsupdates für Betriebssysteme und Systemkomponenten
- Dokumentation der durchgeführten Updates

4. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Datenschutzmanagement
- Formalisierte Prozesse für Datenschutzvorfälle
- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement

5. Ergänzende Maßnahmen für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

Soweit der Auftragnehmer im Rahmen der Auftragsverarbeitung besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO verarbeitet, gelten ergänzend zu den vorstehenden Maßnahmen die folgenden zusätzlichen Schutzmaßnahmen:

a) Datenminimierung

Die Erhebung besonderer Kategorien personenbezogener Daten ist auf das für den jeweiligen Verarbeitungszweck erforderliche Minimum beschränkt. Soweit technisch umsetzbar, werden ausschließlich kategoriale Angaben (z. B. ja/nein) statt Freitextfelder verwendet.

b) Zugriffsbeschränkung nach dem Need-to-know-Prinzip

Der Zugriff auf besondere Kategorien personenbezogener Daten ist auf diejenigen Mitarbeiter des Auftragnehmers beschränkt, die diesen Zugriff zur Erfüllung ihrer konkreten Aufgabe zwingend benötigen. Die Zugriffsberechtigung wird individuell vergeben und dokumentiert.

c) Organisatorische Maßnahmen

Mitarbeiter mit Zugriff auf besondere Kategorien personenbezogener Daten erhalten über die allgemeine Unterweisung hinaus eine vertiefte Schulung zu den erhöhten Schutzanforderungen, der besonderen Vertraulichkeit dieser Daten sowie den spezifischen Verarbeitungsrestriktionen nach Art. 9 DSGVO. Die Zugriffsberechtigungen werden regelmäßig auf ihre fortbestehende Erforderlichkeit überprüft und bei Wegfall des Zugriffsgrunds unverzüglich entzogen.

6. Hetzner Online Sicherheitskonzepte

Für das Hosting der Serverinfrastruktur werden Dedicated Server der Hetzner Online GmbH genutzt. Die Datenverarbeitung erfolgt ausschließlich an Rechenzentrumsstandorten innerhalb Deutschlands (Nürnberg, Falkenstein/Vogtland). Hetzner implementiert insbesondere folgende Sicherheitsmaßnahmen:

a) Physische Sicherheit und Verfügbarkeit

- Elektronisches Zutrittskontrollsystem mit Protokollierung, Hochsicherheitszäune mit Übersteig- und Untergrabenschutz, flächendeckende Videoüberwachung
- Unterbrechungsfreie Stromversorgung durch redundante USVs und Netzersatzanlagen bei redundanter Stromeinspeisung vom Umspannwerk
- Flächendeckende Brandfrüherkennungsmechanismen mit automatischer Alarmierung und Leitstellenanbindung
- Redundante und hochverfügbare Netzwerkinfrastruktur (99,9 % Verfügbarkeit gemäß AGB) mit dauerhaft aktiver DDoS-Erkennung

b) Datenträger und Löschung

- Definierte Verfahren zur Löschung von Festplattendaten nach Auftragsbeendigung; physische Zerstörung von Datenträgern bei nicht erfolgreicher Datenlöschung
- Transport von Datenträgern standortübergreifend ausschließlich in verschlossenen Transportboxen

c) Zertifizierungen und Prüfungen

- ISO/IEC 27001
- BSI C5 Typ 2
- Jährliche Überprüfung der TOMs durch externen Dienstleister

7. DigitalOcean Sicherheitskonzepte

Für das Hosting der Daten wird der Service von DigitalOcean genutzt. DigitalOcean implementiert umfassende Sicherheitsmaßnahmen, insbesondere:

a) Infrastruktursicherheit

- 24/7/365 Überwachung der Infrastruktur über mehrere fehlerunabhängige Verfügbarkeitszonen
- Regelmäßige Drittanbieter-Audits und gezielte Tests

- Physische Sicherheit mit biometrischen Zugangssystemen und Videoüberwachung in allen Rechenzentren

b) Datensicherheit

- Verschlüsselung der Datenbanken mit Advanced Encryption Standard (AES)
- TLS v1.2 für Datenübertragung zwischen Kundenanwendung und DigitalOcean
- Echtzeit-Erkennung und Umleitung bei Problemen mit Hosts oder Rechenzentren

c) Zertifizierungen und Compliance

- AICPA SOC 2 (Typ II) und SOC 3 (Typ II)
- Cloud Security Alliance (CSA) STAR Level 1
- GDPR-konform mit transparenten Datenschutz- und Sicherheitskontrollen
- Regelmäßige interne und externe Sicherheitsaudits

Anlage B: Modulbezogene Aufschlüsselung der Verarbeitungstätigkeiten

Die nachfolgende Aufschlüsselung dient ausschließlich der datenschutzrechtlichen Dokumentation der Verarbeitungstätigkeiten, die im Rahmen der Bereitstellung der twinwin Plattform anfallen können. Sie stellt keine Vereinbarung über den geschuldeten Leistungsumfang dar. Welche Module dem Auftraggeber tatsächlich zur Verfügung stehen und damit Gegenstand der Auftragsverarbeitung sind, richtet sich ausschließlich nach dem Hauptvertrag.

1. Allgemeine Plattformverarbeitung

Die twinwin Plattform verarbeitet im Rahmen der nachfolgend genannten Funktionsbereiche personenbezogene Daten im Auftrag des Auftraggebers:

Feld	Beschreibung
Funktionsbereiche	Plattformzugang und Nutzerverwaltung; Nutzer- und Unternehmensprofile; Interaktionsdaten und Nutzungsverlauf; Nutzung der allgemeinen Module (u. a. Vorlagen, Learning und Events, Entgelttransparenz, Scheinselbstständigkeitsprüfung)
Kategorien betroffener Personen	Mitarbeiter des Auftraggebers (Plattformnutzer); Ansprechpartner und Vertretungsberechtigte des Auftraggebers; eingeladene, noch nicht registrierte Personen; Freelancer / freie Mitarbeiter des Auftraggebers (nur abstrakte Angaben); sonstige Personen, deren Daten der Auftraggeber im Rahmen der Plattformnutzung eingibt
Kategorien personenbezogener Daten	Personenstammdaten, Kontaktdaten, Zugangsdaten, Rollen und Berechtigungen, Nutzungsdaten, Unternehmensdaten, Anmeldedaten zu Events
Rechtsgrundlage des Auftraggebers	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung); Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Nutzung und Sicherheit der Plattform)
Besondere Hinweise	Jeder Nutzer sieht ausschließlich seine eigenen Daten; der Administrator erhält standardmäßig nur aggregierte Statistiken ohne Personenbezug. Auf ausdrückliche Weisung des Auftraggebers und unter der Bedingung einer entsprechenden Erweiterung des Hauptvertrags kann eine erweiterte Sichtbarkeit eingerichtet werden. Die mit der

	Leistungserbringung befassten Mitarbeiter des Auftragnehmers können auf nutzerbezogene Plattformdaten zugreifen, soweit dies zu diesem Zweck erforderlich ist. Soweit der Auftraggeber im Rahmen der Plattformnutzung personenbezogene Daten sonstiger Personen eingibt, liegt die Verantwortung für die Zulässigkeit dieser Eingabe und die Information der betroffenen Personen ausschließlich beim Auftraggeber.
Browserbasierte Verarbeitungen	Einige Funktionen der Plattform verarbeiten personenbezogene Daten der Beschäftigten des Auftraggebers ausschließlich lokal im Browser des Nutzers. Diese Daten werden dabei weder an Server des Auftragnehmers übermittelt noch vom Auftragnehmer gespeichert. Hierzu gehören insbesondere das ETRL Compliance-Modul sowie die ETRL Gehaltsanalyse aus dem Bereich Entgelttransparenz. Für diese rein browserseitige Verarbeitung ist der Auftragnehmer nicht Auftragsverarbeiter; die datenschutzrechtliche Verantwortung verbleibt vollständig beim Auftraggeber.
Eigenverantwortliche Nutzung anonymisierter Daten	Der Auftragnehmer ist berechtigt, Daten, die im Rahmen der Auftragsverarbeitung anfallen, in vollständig anonymisierter Form zu eigenen Zwecken zu verwenden, wie etwa zur Weiterentwicklung der Plattform oder zur Entwicklung und Verbesserung KI-gestützter Funktionen. Die Anonymisierung erfolgt so, dass weder ein Personen- noch ein Unternehmensbezug herstellbar ist. Für die anonymisierten Daten findet die DSGVO keine Anwendung; die Auftragsverarbeitung endet mit dem Abschluss der Anonymisierung. Der Auftragnehmer erteilt dem Auftraggeber auf Anfrage Auskunft über die angewandten Anonymisierungsverfahren und deren Eignung zur irreversiblen Aufhebung des Personenbezugs. Die Auskunft erfolgt in allgemeiner Form und begründet keinen Anspruch auf Offenlegung von Geschäftsgeheimnissen oder proprietären Verfahren.

Die unter dieser Ziffer genannten, allgemeinen Datenkategorien, betroffenen Personen und Hinweise gelten ergänzend auch für alle nachfolgend näher beschriebenen Module.

2. Modul „Frage & Antwort“

Feld	Beschreibung
Zweck	Datenbankbasierte Bereitstellung arbeitsrechtlicher Informationen zu Freitext-Anfragen der Plattformnutzer; Statusverfolgung und Eskalation; Team-Sharing
Kategorien betroffener Personen	Mitarbeiter des Auftraggebers (Plattformnutzer); ggf. in der Anfrage in Bezug genommene Beschäftigte des Auftraggebers
Kategorien personenbezogener Daten	Anfragetext, Antworttexte, Kategorie, Zeitstempel, Status-Historie
Besondere Hinweise	Die Nutzung des Moduls erfolgt über Freitext-Anfragen. Eine Eingabe personenbezogener Daten Dritter ist weder vorgesehen noch erforderlich; im Einzelfall kann jedoch nicht ausgeschlossen werden, dass betroffene Personen aus dem Sachverhalt identifizierbar sind, einschließlich besonderer Kategorien im Sinne von Art. 9 DSGVO (z. B. Gesundheit, Schwerbehinderung). Die Verantwortung für die Zulässigkeit der eingegebenen Inhalte liegt beim Auftraggeber.

3. Modul „Arbeitszeugnisse“

Feld	Beschreibung
Zweck	Erstellung und Verwaltung von Arbeitszeugnissen im Auftrag des Auftraggebers
Kategorien betroffener Personen	Beschäftigte, freie Mitarbeiter und Praktikanten des Auftraggebers (in der Regel keine Plattformnutzer)
Kategorien personenbezogener Daten	Personenstammdaten, Beschäftigungsdaten (Position, Abteilung, Tätigkeitsbeschreibung, Beschäftigungsdauer), Leistungs- und Verhaltensbeurteilung
Besondere Datenkategorien (Art. 9 DSGVO)	In der Regel nicht betroffen. Sollten im Einzelfall besondere Kategorien personenbezogener Daten in Freitextfeldern eingegeben werden, erfolgt die Verarbeitung ausschließlich auf Weisung des Auftraggebers.

Rechtsgrundlage des Auftraggebers	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG
Besondere Hinweise	Die Information der betroffenen Beschäftigten gemäß Art. 13/14 DSGVO obliegt dem Auftraggeber (vgl. § 5 Abs. 2).

4. Modul „Trennungs-Risiko“

Feld	**Beschreibung**
Zweck	Bewertung von Kündigungsrisiken und Erstellung von Trennungsszenarien im Auftrag des Auftraggebers
Kategorien betroffener Personen	Beschäftigte des Auftraggebers (in der Regel keine Plattformnutzer)
Kategorien personenbezogener Daten	Personenstammdaten, Beschäftigungsdaten, Angaben zu Kündigungsgründen und Kündigungsschutz
Besondere Datenkategorien (Art. 9 DSGVO)	Ja. Dieses Modul erfasst im Rahmen der Prüfung des Sonderkündigungsschutzes das Vorliegen besonderer Kategorien personenbezogener Daten, insbesondere: Vorliegen einer Schwerbehinderung (ja/nein), Schwangerschaft oder Mutterschutz (ja/nein), Elternzeit / Pflegezeit (ja/nein), Betriebsratszugehörigkeit (ja/nein). Es werden ausschließlich die für die Beurteilung des Kündigungsschutzes erforderlichen Angaben zum Vorliegen dieser Merkmale erfasst, jedoch keine weitergehenden Details (insbesondere keine Diagnosen, Befunde oder Gesundheitsakten). Die Verantwortung für die Zulässigkeit und Richtigkeit der eingegebenen Daten sowie für die Information der betroffenen Beschäftigten liegt ausschließlich beim Auftraggeber. Die Verarbeitung erfolgt ausschließlich auf Weisung des Auftraggebers.
Rechtsgrundlage des Auftraggebers	Art. 6 Abs. 1 lit. b DSGVO i. V. m. § 26 BDSG; für besondere Kategorien: Art. 9 Abs. 2 lit. b DSGVO i. V. m. § 26 Abs. 3 BDSG
Besondere Hinweise	Aufgrund der Verarbeitung besonderer Datenkategorien gelten erhöhte Schutzmaßnahmen gemäß Art. 32 DSGVO.

5. Modul „Anwalt anfragen“

Feld	Beschreibung
Zweck	Vermittlung arbeitsrechtlicher Beratung durch Partneranwälte und -kanzleien
Kategorien betroffener Personen	Mitarbeiter des Auftraggebers (Plattformnutzer); ggf. in der Anfrage beschriebene Beschäftigte
Kategorien personenbezogener Daten	Anfragetext, Kontaktdaten; sofern vom Nutzer ausgewählt: Kontext aus vorangegangenen Anfragen
Besondere Hinweise	Der Nutzer veranlasst die Weitergabe seiner Anfragedaten an einen Anwalt aus dem Netzwerk des Auftragnehmers. Das Matching erfolgt nach Fachgebiet und Verfügbarkeit. Mit Abschluss der Mandatsvereinbarung wird der Anwalt eigenständig Verantwortlicher (Art. 4 Nr. 7 DSGVO); der Auftragnehmer ist für die anschließende Verarbeitung durch den Anwalt nicht verantwortlich. Auf Veranlassung des Nutzers können auch Kontext-Daten aus anderen Modulen weitergegeben werden.

Der Auftragnehmer verarbeitet darüber hinaus bestimmte Daten in eigener Verantwortlichkeit (Art. 4 Nr. 7 DSGVO). Hierüber informiert der Auftragnehmer die betroffenen Personen in seiner Datenschutzerklärung.