AVV - 16.06.2026 - Electus GmbHVertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen Ihnen als Kunde bei der Electus GmbH als Verantwortlicher
(soweit gewünscht, bitte Anschrift eintragen)

_____
_____
vertreten durch: _____

(nachfolgend Auftraggeber genannt)

und dem Auftragsverarbeiter

Electus GmbH
Rheinpromenade 11, 40789 Monheim am Rhein
vertreten durch: Marlon Pollmeier

(nachfolgend Auftragnehmer genannt)

§ 1 Einleitung

1. Dieser Vertrag regelt das Auftragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer über die Verarbeitung personenbezogener Daten durch den Auftragnehmer. Er begründet das Rechtsverhältnis der Auftragsverarbeitung nach Art. 28 DSGVO.
2. Der Auftragnehmer verarbeitet als Auftragsverarbeiter (Art. 4 Nr. 2 DSGVO) personenbezogene Daten für den Auftraggeber. Diese Dienstleistungen werden auf Grundlage des zwischen den Parteien bestehenden, im folgenden bezeichneten Hauptvertrags erbracht.
3. Der Vertrag bezieht sich auf alle Tätigkeiten des Auftragnehmers, seiner Mitarbeiter und seiner Subunternehmer, bei denen es zur Verarbeitung von personenbezogenen Daten oder zur Berührung mit solchen personenbezogenen Daten kommt, die der Auftragnehmer vom Auftraggeber zur Verfügung gestellt bekommen hat.

§ 2 Auftragsgegenstand und -dauer

1. Der Gegenstand des Auftrags ergibt sich aus dem geschlossenen Vertrag vom _____, auf welche(n) / welches hierdurch verwiesen wird (nachstehend Hauptvertrag genannt).
2. Die Dauer der Auftragsverarbeitung richtet sich nach dem Hauptvertrag und endet bei unbestimmter Laufzeit durch Kündigung des Haupt- oder diesen Vertrags.

§ 3 Auftragsinhalt

1. Die Verarbeitung dient folgendem Zweck:
   Generierung von Bewerbungen für den Auftraggeber, durch Social-Media Werbeanzeigen.
2. Folgende Verarbeitungsvorgänge gem. Art. 4 Nr. 2 DSGVO personenbezogener Daten finden Anwendung:
   - Erheben
   - Erfassen
   - Organisieren
   - Speichern
   - Verwenden

3. Die Verarbeitung erfolgt grundsätzlich in einem Mitgliedstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Einzelne in Anlage 2 benannte Auftragsverarbeiter mit Sitz in einem Drittland (insbesondere den USA) verarbeiten personenbezogene Daten teilweise außerhalb der EU/des EWR oder ermöglichen einen Zugriff aus einem Drittland; die Datenhaltung erfolgt, soweit in Anlage 2 angegeben, innerhalb der EU. Die Übermittlung in ein Drittland ist abgesichert durch:
   - Angemessenheitsbeschluss der Kommission nach Art. 45 DSGVO (insbesondere EU-US Data Privacy Framework) sowie Standardvertragsklauseln nach Art. 46 DSGVO

4. Folgende Datenkategorien werden durch den Auftragnehmer verarbeitet:
   - Personenstammdaten
   - Kommunikationsdaten

   - Bewerbungs- und Qualifikationsdaten (z. B. Lebenslauf, Zeugnisse, optionales Bewerbungsfoto)
   - Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO werden nicht aktiv erhoben; geben betroffene Personen solche Daten freiwillig an, werden diese nur im erforderlichen Umfang verarbeitet.

5. Die Verarbeitung betrifft die Daten folgender Personengruppen des Auftraggebers:
    - Interessenten
    - Andere / weitere Personengruppen: Bewerber

6. Rechtsgrundlage der Verarbeitung für den Auftraggeber ist nach Art. 6 DSGVO:
    - Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben (Art. 6 Abs. 1 lit. a DSGVO)
    - Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 lit. b DSGVO)

§ 4 Umgang mit den Daten, Weisungsrecht des Auftraggebers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich gemäß dieser vertraglichen Vereinbarung oder nach Weisungen des Auftraggebers. Etwas anderes gilt bei einer gesetzlichen oder behördlichen Verpflichtung des Auftragnehmers zu einer anderweitigen Verarbeitung. Dann hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Kenntnis zu setzen. Eine Verarbeitung personenbezogener Daten des Auftraggebers zu eigenen Zwecken des Auftragnehmers ist ausgeschlossen.
2. Der Auftragnehmer verpflichtet sich, die Anforderungen des Auftragsverarbeiters nach Art. 28 und 32 DSGVO sicherzustellen und den diesbezüglichen Nachweis dem Auftraggeber zu erbringen.
3. Der Auftragnehmer verpflichtet sich, diesen Grundsätzen auch dadurch zu genügen, dass er sein Personal ausreichend in Fragen des Datenschutzes schult und entsprechend nur fachkundiges Personal in Kontakt mit den Daten des Auftraggebers treten lässt. Die zur Verarbeitung eingesetzten Beschäftigten des Auftragnehmers werden zur Vertraulichkeit verpflichtet.
4. Der Auftragnehmer verpflichtet sich zur Einhaltung der Regeln zum Datenschutz und bestätigt die Kenntnis dieser einschlägigen Regelungen zur ordnungsgemäßen Verarbeitung personenbezogener Daten. Er ergreift die erforderlichen technisch-organisatorischen Maßnahmen, um eine ordnungsgemäße Verarbeitung sicherzustellen (siehe § 7).
5. Der Auftragnehmer darf personenbezogene Daten, die er im Auftrag des Auftraggebers verarbeitet, nicht eigenmächtig und nur nach dessen Anweisungen berichtigen, löschen, portieren oder beauskunften oder deren Verarbeitung einschränken. Dies gilt auch dann, wenn eine betroffene Person einen entsprechenden Antrag stellt.
6. Die dem Auftragnehmer vom Auftraggeber zur Verfügung gestellten Daten sind unter strikter Trennung von anderen Datenbeständen zu verarbeiten.

7. Der Auftragnehmer darf keine Kopien der zur Verfügung gestellten Daten ohne Wissen des Auftraggebers erstellen. Eine Ausnahme gilt für technisch notwendige und im Rahmen einer ordnungsgemäßen Verarbeitung erforderliche Vervielfältigungen, bei denen eine Gefährdung der Rechte der betroffenen Personen und eine Absenkung des Datenschutzniveaus ausgeschlossen ist.
8. Der Auftragnehmer stellt die Erfüllung der Rechte auf Auskunft, Berichtigung, Einschränkung, Löschung sowie Datenportabilität sicher. Dies gilt unabhängig vom Leistungsumfang des Vertrags. Der Auftragnehmer unterstützt den Auftraggeber umfassend bei der Erfüllung dieser Rechte gemäß Art. 28 Abs. 3 lit. e DSGVO..

§ 5 Sonstige Pflichten des Auftragnehmers und Qualitätssicherung

1. Der Auftragnehmer hat zusätzlich gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; darüber hinaus gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
    1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt, falls rechtlich erforderlich.
    2. Der Auftragnehmer organisiert den Datenschutz durch den Datenschutzbeauftragten:
       Triades Managementberatung
       Inhaber: Martin Lorenz
       Am Hang 8
       31655 Stadthagen

       Fon: +49 (0) 5721/ 8984114
       Fax: +49 (0) 5721/ 8984113

       E-Mail: info@triades-datenschutz.de
    3. Die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO ist zu wahren. Beschäftigte des Auftragnehmers, die er zur Durchführung der Verarbeitung bestellt, müssen zur Vertraulichkeit verpflichtet und mit den für sie zu beachtenden Vorschriften zum Datenschutz vertraut gemacht werden. Der Auftragnehmer und alle ihm unterstellten Personen, die Zugang zu personenbezogenen Daten des Auftraggebers haben, verarbeiten diese ausschließlich gemäß den Weisungen des Auftraggebers und den Bestimmungen dieses Vertrags, sofern gesetzlich keine anderweitigen vorgaben bestehen. Die Vertraulichkeitsregeln gelten nach Beendigung des Vertrags fort.

4. Die Einhaltung der für diesen Auftrag erforderlichen organisatorischen und technischen Maßnahmen nach Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (siehe Anlage 1).
5. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf Gegenstände dieses Vertrags beziehen. Dies gilt auch bei Ermittlungen der zuständigen Aufsichtsbehörde in einem Straf- oder Ordnungswidrigkeitsverfahrens, das die Verarbeitung personenbezogener Daten aufgrund dieses Vertragsverhältnisses betrifft.
6. Auftraggeber und Auftragnehmer verpflichten sich zur Zusammenarbeit mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben.
7. Der Auftragnehmer ist verpflichtet, in regelmäßigen Abständen die internen Prozesse und die technischen und organisatorischen Maßnahmen zu kontrollieren. Dadurch soll gewährleistet werden, dass sich die Verarbeitung stets im Einklang mit dem geltenden Datenschutzrecht befindet und die Rechte der betroffenen Person geschützt sind.
8. Unterliegt der Auftraggeber einer Kontrolle oder Maßnahme der Aufsichtsbehörde, einem Straf- oder Ordnungswidrigkeitsverfahren, Haftungsansprüchen oder anderen Ansprüchen betroffener oder dritter Personen im Zusammenhang mit der Auftragsverarbeitung im Rahmen dieses Vertragsverhältnisses, ist der Auftragnehmer verpflichtet, den Auftraggeber nach besten Kräften zu unterstützen.
9. Der Auftragnehmer hat die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber nach dessen Kontrollbefugnissen nach § 8 dieses Vertrags nachzuweisen.

§ 6 Unterauftragsverhältnisse

1. Der Auftraggeber erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 2 genannten Subunternehmer als weitere Auftragsverarbeiter. Beabsichtigt der Auftragnehmer, einen weiteren Subunternehmer hinzuzuziehen oder einen bestehenden zu ersetzen, teilt er dies dem Auftraggeber mindestens vier Wochen vorab in Textform mit. Der Auftraggeber kann der Änderung innerhalb von zwei Wochen ab Zugang der Mitteilung aus einem datenschutzrechtlich begründeten Anlass widersprechen. Widerspricht der Auftraggeber nicht fristgerecht, gilt die Änderung als genehmigt. Im Fall eines Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung; kommt diese nicht zustande, ist jede Partei berechtigt, den Vertrag zu kündigen. Ein Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer den Dritten mit der vollständigen oder teilweisen Erfüllung dieses Vertrags beauftragt. Erforderlich ist, dass die Tätigkeiten des Subunternehmers in

unmittelbarem Zusammenhang mit der Hauptleistung dieses Vertrags stehen. Nebenleistungen wie der Transport, die Bewachung oder die Reinigung stellen keine Unterauftragsverhältnisse in diesem Sinn dar.

2. Die Auswahl des Subunternehmers ist unter Berücksichtigung der Voraussetzungen des Art. 28 DSGVO und den Standards dieses Vertrags durch den Auftragnehmer zu treffen. Die Eignung des Subunternehmers zur ordnungsgemäßen Datenverarbeitung und zur Einhaltung der technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO ist zu gewährleisten. Der Auftragnehmer stellt sicher, dass dem Subunternehmer im Hinblick auf das Schutzniveau der personenbezogenen Daten solche Verpflichtungen auferlegt werden, die mit den in diesem Vertrag begründeten Anforderungen vergleichbar sind. Der Auftragnehmer verpflichtet sich außerdem, regelmäßig zu überprüfen und zu dokumentieren, ob das erforderliche Datenschutzniveau der Subunternehmer in Drittländern eingehalten wird. Die Ergebnisse dieser Überprüfungen sind dem Auftraggeber auf Verlangen vorzulegen. Der Auftragnehmer hat dem Auftraggeber die Kontaktdaten des Subunternehmers sowie eine Beschreibung der Datenverarbeitungsprozesse zu übermitteln.
3. Der Auftragnehmer stellt sicher, dass die aus diesem Vertrag oder dem Gesetz folgenden Rechte des Auftraggebers auch im Verhältnis zum Subunternehmer wirksam ausgeübt werden können.
4. Die Kontrolle des Subunternehmers durch den Auftragnehmer gestaltet sich nach den in diesem Vertrag geregelten Grundsätzen zur Kontrolle des Auftragnehmers durch den Auftraggeber. Der Auftragnehmer hat regelmäßige Kontrollen durchzuführen und die Ergebnisse zu dokumentieren und dem Auftraggeber auf Verlangen vorzulegen. Der Nachweis der Kontrollmaßnahmen kann erfolgen durch:
    - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
    - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
    - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
    - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz)

    Der Beauftragung der in Anlage 2 zu diesem Vertrag aufgeführten Subunternehmer stimmt der Auftraggeber unter Einhaltung der vorstehenden Voraussetzungen zu. Die jeweils aktuelle Liste der genehmigten Subunternehmer ergibt sich aus Anlage 2.

§ 7 Technisch- organisatorische Maßnahmen (TOMs)

1. Der Auftragnehmer hat bei seinen Verarbeitungstätigkeiten ein Schutzniveau zu gewährleisten, dass eine Gefährdung für die Rechte und Freiheiten der betroffenen Personen ausschließt. Alle Tätigkeiten des Auftragnehmers müssen sich im Einklang mit der des Art. 28 i.V.m. Art. 5 I DSGVO sowie des Art. 32 DSGVO zur Sicherheit der Verarbeitung halten. Dafür verpflichtet sich der Auftragnehmer, die in der Anlage 1 aufgeführten technisch-organisatorischen Maßnahmen, die in seinem Verantwortungsbereich liegen, einzuhalten. Der Auftragnehmer übergibt dem Auftraggeber eine entsprechende Dokumentation vor Beginn der Verarbeitung zum Audit / Prüfung.
2. Die vereinbarten technisch-organisatorischen Maßnahmen unterliegen der durch den technischen Fortschritt bedingten Weiterentwicklung. Insofern darf der Auftragnehmer in der Zukunft alternative adäquate Maßnahmen ergreifen, wenn damit keine Absenkung des Sicherheitsniveaus der festgelegten Maßnahmen verbunden ist.

§ 8 Kontrollrechte des Auftraggebers

1. Der Auftraggeber kann, die Einhaltung der Vorschriften über den Datenschutz und der Vorgaben dieses Vertrags durch Kontrollen feststellen. Die Kontrollen können auch von Dritten durchgeführt werden, die der Auftraggeber nach seinem Ermessen bestimmt. Der Auftragnehmer hat das Recht, die Kontrolle durch den Dritten bei Vorliegen besonderer Umstände abzulehnen (oder z.B. Bestehen eines Wettbewerbsverhältnisses zwischen Auftragnehmer und Drittem). Der Auftragnehmer ist verpflichtet, den Auftraggeber bei den Kontrollen nach seinen Kräften zu unterstützen, indem er unter anderem die erforderlichen Auskünfte gibt, Einsicht in seine Unterlagen gewährt und Zutritt zu seinen Räumlichkeiten gewährt.
2. Bei Ermöglichung der Kontrollen durch den Auftraggeber wird der Auftragnehmer keinen Vergütungsanspruch geltend machen.
3. Der Auftraggeber muss die Kontrollen in der Regel in einem angemessenen zeitlichen Abstand ankündigen. Sie sind in einem angemessenen Rahmen und mit Rücksicht auf die Interessen des Auftragnehmers durchzuführen, soweit der Auftragnehmer nicht nach § 6 (5) dieses Vertrages die Kontrollen durch dort genannte Nachweise (durch Kontrollen unabhängiger Dritter) abwendet. Dies schließt ein, dass sie zu den gewöhnlichen Geschäftszeiten des

Auftragnehmers stattfinden und den ordentlichen Geschäftsablauf soweit möglich nicht übermäßig stören.

§ 9 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

1. Der Auftragnehmer hat den Auftraggeber im Fall einer vertragswidrigen, gesetzeswidrigen oder anderweitig rechtswidrigen Verarbeitung durch den Auftragnehmer oder durch bei ihm beschäftigte Personen unverzüglich zu informieren. Dies gilt auch, wenn lediglich ein Verdacht einer Datenschutzverletzung besteht sowie bei festgestellten Unregelmäßigkeiten. Das weitere Vorgehen wird vom Auftraggeber und Auftragnehmer einvernehmlich bestimmt.
2. Der Auftragnehmer hat den Auftraggeber bei der Erfüllung seiner datenschutzrechtlichen Pflichten nach Art. 28 III (f) DSGVO, insbesondere bei der Erfüllung nach den Art. 32-36 DSGVO zu unterstützen.

§ 10 Weisungsbefugnisse des Auftraggebers

1. Der Auftraggeber hat im Hinblick auf die durchzuführenden Verarbeitungstätigkeiten ein umfassendes Weisungsrecht. Die Erteilung einer Weisung ist vom Auftragnehmer unverzüglich zu bestätigen.
2. Ausschließlich die folgenden Personen sind zur Erteilung und zur Annahme von Weisungen befugt. Ein Wechsel der Personen ist der jeweils anderen Vertragspartei unverzüglich mitzuteilen.

   Erteilung von Weisungen:

   _____
   _____

   Annahme von Weisungen:

   Marlon Pollmeier
   mp@electus.de

3. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen Datenschutzvorschriften oder Vorschriften dieses Vertrags verstößt, hat er den Auftraggeber unverzüglich darüber zu informieren. Er darf die Durchführung der Weisung so lange unterlassen, wie der Auftraggeber sie nicht bestätigt, geändert oder widerrufen hat. Mündliche Weisungen sind ausgeschlossen.

§ 11 Verpflichtungen nach Beendigung des Auftragsverhältnisses

1. Die Verpflichtungen ergeben sich aus dem Hauptvertrag und ggf. dem Gesetz. Nach Vertragsbeendigung im Besitz des Auftragnehmers befindliche Daten sind nach Wahl des Auftraggebers an diesen zurückzugeben oder zu vernichten. Der Auftraggeber kann den Auftragnehmer zur Wahl auffordern. Die Vernichtung hat in einer mit der DSGVO konformen Weise zu erfolgen, die die Wiederherstellung der Daten ausschließt. Die ordnungsgemäße Vernichtung ist vom Auftragnehmer nachzuweisen.
2. Selbige Anforderungen gelten auch im Verhältnis des Auftragnehmers zu seinen Subunternehmern.
3. Der Auftragnehmer ist verpflichtet, alle Dokumentationen, die dem Beleg der Rechtmäßigkeit der Vereinbarung dienen, nach dem Vertragsende für die Dauer von 12 Monaten aufzubewahren. Wahlweise kann er sie dem Auftraggeber übergeben.

§ 12 Telearbeit beim Auftragnehmer

1. Der Auftragnehmer ist berechtigt, seinen Beschäftigten Telearbeit anzubieten. Er schließt mit ihnen eine betriebliche Vereinbarung über die Telearbeit, die die Einhaltung aller Vorschriften zum Datenschutz und zur Datensicherheit sicherstellt.
2. Eine Gefährdung der Daten muss ausgeschlossen sein. Die Sicherheit der Daten ist insbesondere durch einen sicheren Dienstrechner und das Einrichten einer verschlüsselten Verbindung zu gewährleisten.

§ 13 Betroffenenrechte

1. Macht eine betroffene Person Rechte gegenüber dem Auftragnehmer geltend, hat dieser die Person unverzüglich an den Auftraggeber zu verweisen und den Antrag an diesen weiterzuleiten. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Ansprüchen betroffener Personen in angemessenem Umfang (Art. 28 III lit. e, f DSGVO).
2. Der Auftragnehmer verpflichtet sich, Weisungen des Auftraggebers Folge zu leisten, die den Inhalt haben, dass Daten aus dem Auftragsverhältnis zu löschen, zu berichtigen, deren Verarbeitung einzuschränken ist. Dies gilt nicht, wenn berechtigte Interessen des Auftragnehmers entgegenstehen.
3. Auskünfte über personenbezogene Daten darf der Auftragnehmer nicht ohne vorherige Zustimmung oder Weisung des Auftraggebers an Dritte erteilen.
4. Als Rechte des Betroffenen gemäß dieses Abschnitts kommen die folgenden in Betracht:
    - Art. 7 III, 8 DSGVO bzw. § 7 UWG und/oder § 203 StGB: Widerruflichkeit der Einwilligung
    - Art. 15 DSGVO: Recht auf Auskunft über die verarbeiteten personenbezogenen Daten

- Art. 16 DSGVO: Recht auf Vervollständigung bzw. Berichtigung der verarbeiteten personenbezogenen Daten
- Art. 17 DSGVO: Recht auf Löschung der verarbeiteten personenbezogenen Daten (Recht auf Vergessenwerden)
- Art. 18 DSGVO: Verlangen auf Einschränkung der Verarbeitung personenbezogener Daten
- Art. 20 DSGVO: Recht auf Datenportabilität
- Art. 77 DSGVO: Recht auf Beschwerde bei einer Aufsichtsbehörde
- Art. 34 DSGVO: Recht auf Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten
- Art. 13, 14 DSGVO: Recht auf Information über die Erhebung personenbezogener Daten, die bei der betroffenen Person und nicht bei der betroffenen Person erhoben werden
- Art. 19 DSGVO: Recht auf Mitteilung im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
- Art. 38 IV DSGVO: Recht auf Konsultation des Datenschutzbeauftragten
- § 41 BDSG: Recht auf Konsultation der zuständigen Staatsanwaltschaft
- Art. 82 DSGVO bzw. §§ 280 ff., 823 ff. BGB: Anspruch auf Schadensersatz bei Rechtsverletzung in Bezug auf personenbezogene Daten
- Art. 22: Recht, nicht ausschließlich automatisierten Entscheidungen unterworfen zu werden, das für eine rechtliche oder in ähnlicher Weise erhebliche Beeinträchtigung sorgt
- Art. 12: Recht auf Information über die Rechte nach Art. 13-22, 34 in transparenter Weise

§ 14 Sonstiges

1. Wenn Daten des Auftraggebers oder seines Kunden beim Auftragnehmer oder Subauftragnehmer durch Beschlagnahme oder Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder sonstige Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich hierzu zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich hierzu informieren, dass die Hoheit an den Daten beim Auftraggeber vorliegt.
2. Die Vertragspartner behandeln alle im Rahmen dieses Vertragsverhältnisses erlangten Kenntnisse vertraulich, auch nach Beendigung des Vertragsverhältnisses.
3. Nebenabreden müssen in schriftlicher oder elektronisch dokumentierter Form (z.B. E-Mail) unter Bezugnahme auf diesen Vertrag getroffen werden. Dasselbe

gilt für Änderungen und Ergänzungen dieses Vertrags. Diese müssen die geänderte Regelung ausdrücklich bezeichnen.

4. Individuelle Angaben (Anschrift des Auftraggebers, Datum und Bezeichnung des Hauptvertrags sowie die weisungsberechtigten Personen des Auftraggebers) ergeben sich aus dem Hauptvertrag und sind nicht Bestandteil dieses Anhangs.
5. Dieser Auftragsverarbeitungsvertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen des Auftragnehmers. Der Auftragnehmer kann ihn anpassen, soweit dies aufgrund geänderter rechtlicher Rahmenbedingungen, behördlicher oder gerichtlicher Vorgaben oder geänderter Verarbeitungsabläufe erforderlich ist. Änderungen teilt der Auftragnehmer dem Auftraggeber in Textform mit und weist dabei auf die Frist und die Bedeutung des Schweigens hin. Die Änderungen gelten als angenommen, wenn der Auftraggeber ihnen nicht innerhalb von sechs Wochen ab Zugang der Mitteilung in Textform widerspricht. Widerspricht der Auftraggeber fristgerecht, gilt die bisherige Fassung fort und die Parteien bemühen sich um eine einvernehmliche Lösung.
6. Der Auftragnehmer hat kein Zurückbehaltungsrecht im Hinblick auf die Daten des Auftraggebers und die zugehörigen Datenträger.
7. Sind einzelne Bestandteile dieses Vertrags unwirksam, berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. Bei Vorliegen einer unwirksamen Regelung oder eine Lücke sind diese durch die Regelung zu ersetzen, die die Parteien in Kenntnis der Unwirksamkeit oder der Lücke vereinbart hätten und die der fehlerhaften Regelung möglichst nahekommt.
8. Der Gerichtsstand ist Düsseldorf.
9. Es gilt deutsches Recht.

Dieser Vertrag gilt ohne Unterschriften der Parteien als Bestandteil / Anhang der AGB des Auftragnehmers.

Monheim am Rhein, Stand: 06/2026

Allgemeine technisch organisatorische Maßnahmen

erstellt am

16.06.2026

gültig für folgende Organisation

Electus GmbH
Rheinpromenade 11,
40789 Monheim am Rhein
Deutschland

1.1.1 Vertraulichkeit: Zutrittskontrolle

Bezeichnung	Letztes Audit
1.1.1.03 Zugängliche Fenster und Außentüren der Unternehmensräumlichkeiten sind einbruchssicher ausgeführt	16.06.2026
1.1.1.04 Eingangstüren zu Unternehmensgebäuden oder Räumen sind durch eine genormte Schließanlage gesichert (Sicherheitsschlösser, Chipkarten, Transponder, Codeschloss)	16.06.2026
1.1.1.05 Eingangstüren zu Unternehmensräumlichkeiten weisen neben Schließanlagen, zusätzliche Zutrittssicherungen auf (zb. Türknauf außen)	16.06.2026
1.1.1.06 Die Vergabe, Verlust und Rückgabe von Schlüsseln, Transpondern, Chipkarten oder Codes an Personen wird dokumentiert	16.06.2026
1.1.1.08 Es ist sichergestellt, dass Personen nur dort Zutritt erhalten, wo Sie für die Erfüllung Ihrer Aufgaben auch Zutritt benötigen	16.06.2026
1.1.1.16 Personal von Fremdfirmen das ständig Zugang zu den Unternehmensräumlichkeiten hat (Reinigungskräfte, Sicherheitskräfte, Wartungspersonal), wurde über den Vermieter auf die Geheimhaltung verpflichtet	16.06.2026

1.1.2 Vertraulichkeit: Zutrittskontrolle (sensible Räume)

Bezeichnung	Letztes Audit
1.1..2.04 Personalakten werden in verschließbaren Aktenschränken aufbewahrt	16.06.2026
1.1.2.03 Die Eingangstüren zu Räumen, in denen Personaldaten verarbeitet werden, verfügen über einen automatischen Schließ- und Sperrmechanismus oder werden beim Verlassen versperrt	16.06.2026
1.1.2.15 In sensiblen Räumlichkeiten (Personal, Kundenverwaltung, IT) befinden sich keine Geräte, zu denen ein Benutzerkreis außerhalb der eigentlich Berechtigten Zugang benötigt (zB. Drucker)	16.06.2026

1.2 Vertraulichkeit: Zugangskontrolle

Bezeichnung	Letztes Audit
1.2.02 Laptops oder Smart Devices (Ipad etc.) werden nach Dienstende versperrt aufbewahrt oder werden mit nach Hause genommen	16.06.2026
1.2.05 Die Anmeldung an einem Client erfolgt durch personenbezogene Benutzeraccounts (Benutzername und Passwort oder ähnliche Verfahren (Gesichtserkennung, Fingerprint etc.))	16.06.2026
1.2.06 Die Benutzer:innen am Client Rechner hat keine Administrator Rechte bzw. für die tägliche Arbeit wird mit einem Benutzer:in ohne Administratorrechten gearbeitet	16.06.2026
1.2.07 Sammelaccounts oder unpersonalisierte Benutzerzugänge auf Clients (mehrere Benutzer teilen sich einen Zugang) existieren nicht	16.06.2026
1.2.08 Auf jedem verwendeten Client (Rechner) ist eine Firewall aktiv	16.06.2026
1.2.09 Auf jedem Client Rechner ist eine Antiviren Software installiert, diese wird täglich bzw. bei einer Neuanmeldung aktualisiert	16.06.2026

Bezeichnung	Letztes Audit
1.2.10 Eingehende Mails werden online am E-Mail Server (beim Hoster) auf Viren geprüft	16.06.2026
1.2.11 Eingehende Mails werden online am Mail Server (Hoster) auf Spam geprüft	16.06.2026
1.2.12 Auf jedem Client Rechner ist eine (Antiviren) Software installiert die beim Surfen im Internet entsprechenden Schutz (Webfilter) bietet	16.06.2026
1.2.14 Der Zugang zum internen Netzwerk (WLAN) ist mit einem eigenen Passwort gesichert	16.06.2026
1.2.16 Der Zugang zur Konfigurationsoberfläche des (WLAN) Routers wurde mit einem eigenen Benutzernamen und einem eigenen Passwort (ungleich Standard Benutzeraccount) gesichert	16.06.2026
1.2.19 Eine Firewall ist auf jedem Übergang zum Internet aktiviert (Router)	16.06.2026
1.2.21 Auf jedem Server und sonstigen Systemen bei denen ein Datenaustausch über das Internet erfolgt ist eine Antiviren Software installiert die täglich aktualisiert wird	16.06.2026
1.2.22 Mobile Endgeräte werden durch den Einsatz einer Antiviren Software geschützt	16.06.2026
1.2.24 Bei Bildschirmen die in Räumlichkeiten eingesetzt werden, zu denen Kund:innen (Patienten:innen...) Zugang haben und personenbezogene Daten verarbeitet werden, wird darauf geachtet, dass der Bildschirm nicht eingesehen werden kann. Allenfalls existiert ein entsprechender Sichtschutz.	16.06.2026
1.2.25 Bildschirme werden automatisch bei Inaktivität gesperrt und können nur durch Eingabe des Benutzerpasswortes oder ähnliche Verfahren (Fingerprint, Gesichtserkennung, etc.) wieder entsperrt werden	16.06.2026

1.3 Vertraulichkeit: Zugriffskontrolle

Bezeichnung	Letztes Audit
1.3.01 Die Anzahl der Administratoren für Server und zentrale Software ist auf das „Notwendigste“ reduziert	16.06.2026
1.3.02 Jeder Administrator verfügt über einen eigenen Benutzeraccount und das Passwort besteht zumindest aus 12 Stellen	16.06.2026
1.3.05 Passwörter von Benutzer:innen weisen eine ausreichende Komplexität auf (beinhalten Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern und weisen eine Mindestlänge von 8 Stellen auf)	16.06.2026
1.3.06 Die Verwaltung von Benutzerrechten für genutzte Software erfolgt zentral über festgelegte Systemadministratoren	16.06.2026
1.3.07 Jeder User erhält für jedes System und jede Software die er für seine Tätigkeit benötigt einen eigenen Benutzeraccount (keine Sammelaccounts)	16.06.2026
1.3.08 Jeder User erhält auf Basis des "need to know" Prinzip, nur die Zugriffsrechte (auf Daten, Systeme, Software, Dateiablagesysteme) die er für seine Tätigkeit auch zwingend benötigt	16.06.2026
1.3.09 Beim Ausscheiden von Mitarbeiter:innen aus dem Unternehmen ist sichergestellt, dass Zugriffsberechtigungen umgehend entfernt und	16.06.2026

Bezeichnung	Letztes Audit
User in Systemen nach Ablauf einer gewissen Frist auch gelöscht werden.	
1.3.10 Die Vergabe von Zugriffsberechtigungen erfolgt auf Basis von definierten Benutzerprofilen	16.06.2026
1.3.11 Fällt die Notwendigkeit eines oder mehrerer Zugriffsrechte bei einem Benutzer weg, dann werden ihm die Rechte auch zeitnah entzogen	16.06.2026
1.3.12 Zugriffe auf sensible Anwendungen oder Daten werden protokolliert (wer hat wann auf Daten zugegriffen, sie verändert oder gelöscht)	16.06.2026

1.4 Vertraulichkeit: Trennungsgebot

Bezeichnung	Letztes Audit
1.4.02 Bei Softwareapplikationen die personenbezogene Daten verarbeiten existiert eine Trennung in Test- und Produktivsystem	16.06.2026
1.4.03 Der Zugriff auf Daten in Datenbanken ist geregelt	16.06.2026
1.4.05 Softwareapplikationen und Dateiablagen auf die mehrere Benutzer:innen Zugriff haben, sind mit einem Berechtigungssystem ausgestattet.	16.06.2026
1.4.06 Die Verarbeitung von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	16.06.2026
1.4.07 Die Weitergabe von personenbezogenen Daten erfolgt nur zu den festgelegten Zwecken	16.06.2026

1.6 Vertraulichkeit: Verschlüsselung

Bezeichnung	Letztes Audit
1.6.01 Festplatten in Servern werden verschlüsselt	16.06.2026
1.6.02 Festplatten in Laptops / Notebooks werden verschlüsselt	16.06.2026
1.6.03 Mobile Datenträger werden verschlüsselt	16.06.2026
1.6.04 Zur Datenweitergabe werden verschlüsselte Verbindungen wie https (Webseite) oder sftp (FTP Server) genutzt	16.06.2026
1.6.06 Es wird die aktuellste Version des TLS Verschlüsselungsprotokolls verwendet	16.06.2026
1.6.08 Datenbanken in den personenbezogene Daten verarbeitet werden sind verschlüsselt	16.06.2026

2.1 Integrität: 1. Eingabekontrolle

Bezeichnung	Letztes Audit
2.1.01 Dokumente oder Formulare in denen sensible Daten erhoben werden, werden aufbewahrt sofern diese automatisch weiterverarbeitet werden, um Datenfehlübernahmen korrigieren zu können.	16.06.2026
2.1.02 Es existiert eine Übersicht/ Dokumentation, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.	16.06.2026

Bezeichnung	Letztes Audit
2.1.03 Die Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer (nicht Benutzergruppen) kann nachvollzogen werden	16.06.2026
2.1.04 Es erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Daten inkl. Zeitpunkt der Änderung sowie wer die Daten geändert hat	16.06.2026

2.2. Integrität: 2. Weitergabekontrolle

Bezeichnung	Letztes Audit
2.2.01 Die Übermittlung von personenbezogenen Daten zu Lieferanten (Auftragsverarbeiter) erfolgt verschlüsselt (Mailverschlüsselung, VPN Tunnel etc.)	16.06.2026
2.2.03 Auf Rechner wird mittels Fernwartung nur nach Zustimmung des Benutzers zugegriffen. Ausgenommen davon sind Update- und Konfigurationsvorgänge am Rechner mit Hilfe automatischer Installationstools.	16.06.2026
2.2.04 05 Die Daten auf Datenträgern von Laptops oder Desktop-Computern werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.	16.06.2026
2.2.05 Daten auf sonstigen Datenträgern (USB Sticks, mobile Festplatten, ausgebaute Festplatten) werden vor deren internen oder externen Weitergabe gelöscht oder formatiert.	16.06.2026
2.2.06 Bei Druckern oder Faxgeräten werden deren interne Datenträger vor der externen Weitergabe formatiert oder die Daten nach Vorgaben des Herstellers gelöscht	16.06.2026
2.2.08 Für die Aktenvernichtung werden Dienstleister (nach Möglichkeit mit Datenschutz-Gütesiegel) eingesetzt	16.06.2026
Datenträger werden vor der Entsorgung physisch zerstört	16.06.2026

3.1 Verfügbarkeit und Belastbarkeit: Verfügbarkeitskontrolle

Bezeichnung	Letztes Audit
3.1.01 Auf Clients und Servern werden Updates und Sicherheitspatches regelmäßig eingespielt	16.06.2026
3.1.02 Von relevanten Systemen (zB. Buchhaltung, CRM, HR Software) oder sonstigen Systemen die personenbezogene Daten verarbeitet werden, werden regelmäßige Datensicherungen erstellt	16.06.2026
3.1.03 Datensicherungen werden räumlich getrennt von den Produktivdaten aufbewahrt	16.06.2026
3.1.05 Datensicherungen werden nach einem definierten Zeitraum gelöscht	16.06.2026
3.1.06 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, sind mit einer Feuer- und Rauchmeldeanlage ausgestattet	16.06.2026
3.1.07 Räumlichkeiten in denen personenbezogene Daten verarbeitet werden, verfügen leicht erreichbar, über geeignete Löschmittel zur Brandbekämpfung (zB. Feuerlöscher)	16.06.2026

4.1 Verfahren zur Überprüfung: Datenschutz-Management

Bezeichnung	Letztes Audit
4.1.02 Es wird ein Verzeichnis der Verarbeitungstätigkeiten geführt und laufend aktualisiert	16.06.2026
4.1.03 Eine Überprüfung der Wirksamkeit der technisch organisatorischen Maßnahmen findet jährlich statt	16.06.2026
4.1.04 Es existieren Abläufe zur Erfüllung der Rechte von betroffenen Personen	16.06.2026
4.1.05 Eine Datenschutz Management Software ist im Einsatz	16.06.2026
4.1.06 Die Informationspflichten (Datenschutzerklärung) werden regelmäßig geprüft	16.06.2026
4.1.07 Es existiert ein Löschkonzept in dem festgelegt ist, wann, welche Daten zu löschen sind. Die Löschung von Daten wird stichprobenartig oder regelmäßig überprüft.	16.06.2026
4.1.10 Alle Mitarbeiter:innen sind auf Vertraulichkeit und Datengeheimnis verpflichtet	16.06.2026
4.1.11 Mitarbeiter:innen werden jährlich im Bereich Datenschutz geschult bzw. nachweislich sensibilisiert	16.06.2026
4.1.12 Alle Mitarbeiter:innen sind nachweislich geschult, wie sie bei Anfragen von Betroffenen zu Auskunft oder Löschung der Daten vorgehen sollen	16.06.2026
4.1.13 Für die Vergabe von Zugriffsberechtigungen existiert ein Konzept, dass regelmäßig einem Audit unterzogen wird	16.06.2026
4.1.14 Eine Richtlinie zur richtigen Verwendung und Aktualisierung von Passwörtern wurde erstellt und die Mitarbeiter werden dahingehend geschult	16.06.2026
4.1.15 in Bereichen in denen sensible personenbezogene Daten verarbeitet werden existiert eine Clean/ Clear Desk Richtlinie. Die betroffenen Mitarbeiter werden regelmäßig dahingehend sensibilisiert.	16.06.2026
4.1.19 Es existiert eine Richtlinie zum Transport und zur Verwahrung von Laptops und Smart Devices bei Dienstreisen und im Heimbüro	16.06.2026
4.1.20 Mitarbeiter:innen sind angewiesen, die gültigen Datenschutzmaßnahmen auch im Home Office zu gewährleisten	16.06.2026
4.1.21 Um bei Angriffen auf die IT oder Katastrophenfällen geordnet reagieren zu können, haben wir einen Notfallplan erstellt.	16.06.2026

4.2 Verfahren zur Überprüfung: Incident-Response-Management

Bezeichnung	Letztes Audit
4.2.01 Fehlerhafte Login Versuche führen zu einer automatischen Sperre des User Logins. Die Sperre bleibt für einen definierten Zeitraum (siehe Passwort Richtlinie) bestehen.	16.06.2026
4.2.02 Ein Ablauf zur Meldung von Sicherheitsverletzungen an die Datenschutz Behörde und betroffene Personen existiert	16.06.2026
4.2.03 Ein Ablaufplan zum Umgang mit Sicherheitsverletzungen liegt vor	16.06.2026
4.2.04 Jede Sicherheitsverletzung wird an zentraler Stelle dokumentiert und priorisiert	16.06.2026

Bezeichnung	Letztes Audit
4.2.05 Mitarbeiter:innen werden jährlich geschult wie sie mit Sicherheitsverletzungen umgehen sollen	16.06.2026
4.2.06 Zu jeder Sicherheitsverletzung werden Maßnahmen diskutiert und umgesetzt die zu einer Vermeidung oder Milderung weiterer Sicherheitsverletzungen führen (TOMs!)	16.06.2026
4.2.07 Verarbeitungen werden hinsichtlich einer Datenschutz Folgeabschätzung geprüft. Eine solche wird bei Bedarf auch durchgeführt und dokumentiert	16.06.2026

4.4 Verfahren zur Überprüfung: Auftragskontrolle

Bezeichnung	Letztes Audit
4.4.01 Es existiert eine Übersicht über alle Lieferanten (Empfänger), die in unserem Namen personenbezogene Daten als Auftragsverarbeiter verarbeiten	16.06.2026
4.4.02 Die Auswahl von Auftragnehmern erfolgt unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	16.06.2026
4.4.04 Mit all unseren Auftragsverarbeitern haben wir einen Auftragsverarbeitervertrag abgeschlossen	16.06.2026
4.4.05 Es sind wirksame Kontrollrechte gegenüber dem Auftragnehmern vertraglich (Auftragsverarbeitervertrag) vereinbart	16.06.2026
4.4.06 In den Auftragsverarbeiter-Verträgen ist sicher gestellt, dass Daten nach Beendigung des Auftrags auch vernichtet oder übergeben werden	16.06.2026
4.4.07 Wir überprüfen regelmäßig ob unsere Auftragsverarbeiter die festgelegten Datenschutzmaßnahmen einhalten	16.06.2026
4.4.08 Die Wirksamkeit von Datenschutzmaßnahmen oder die Gültigkeit entsprechender Zertifikate werden bei Auftragsverarbeitern regelmäßig geprüft	16.06.2026
4.4.10 Mitarbeiter von Auftragnehmern werden auf das Datengeheimnis verpflichtet bzw. der Auftragnehmer muss dies seinerseits sicher stellen	16.06.2026

Anlage 2: Verzeichnis der genehmigten Subunternehmer (Subprozessoren)

Die nachfolgenden Subunternehmer verarbeiten im Auftrag des Auftragnehmers personenbezogene Daten der betroffenen Personen (Bewerber). Maßgeblich ist die jeweils aktuelle Fassung dieser Anlage. Die angegebenen Firmensitze sind anhand des jeweils mit dem Subunternehmer geschlossenen Auftragsverarbeitungsvertrags zu prüfen.

Subunternehmer	Art und Zweck der Verarbeitung	Verarbeitete Daten	Verarbeitungsstandort / Drittland
Vercel Inc. 340 S Lemon Ave #4133, Walnut, CA 91789, USA	Hosting der Jobseiten (Landingpages), über die Bewerber Stellenanzeigen einsehen und ihre Daten eingeben; Bereitstellung des Frontends der Bewerbermanagement-Plattform.	Name, Telefonnummer, E-Mail-Adresse, optional Lebenslauf	Datenregion Frankfurt (fra1); Unternehmenssitz USA (Drittland). EU-Standardvertragsklauseln / Data Privacy Framework.
Supabase, Inc. [Firmensitz gemäß unterzeichnetem AVV prüfen]	Datenbank-Backend der Bewerbermanagement-Plattform; Speicherung und Verwaltung der Bewerberdaten.	Name, Telefonnummer, E-Mail-Adresse, optional Lebenslauf, Bewerbungsstatus	Datenhaltung EU (Frankfurt); Unternehmenssitz Drittland (USA). EU-Standardvertragsklauseln.
Make (Celonis SE) Theresienstraße 6, 80333 München (Entity gemäß AVV prüfen, ggf. Celonis, Inc., USA)	Automatisierte Übertragung der Bewerberdaten zwischen den Systemen (Webhooks, Workflows).	Name, Telefonnummer, E-Mail-Adresse, optional Lebenslauf (durchlaufend)	Datenhaltung EU-Rechenzentrum. Kein Drittlandtransfer bei Vertragsschluss mit der EU-Gesellschaft (Celonis SE); Entity gemäß AVV prüfen.
Cloudflare, Inc. 101 Townsend Street, San Francisco, CA 94107, USA	Domainverwaltung (DNS), Content Delivery und Sicherheitsfunktionen (Reverse Proxy, DDoS-Schutz) für die bewerberseitige Domain.	Technische Verbindungsdaten (IP-Adresse), durchlaufende Bewerberdaten	Datenhaltung/Region EU (Frankfurt); globales Netzwerk; Unternehmenssitz USA (Drittland). EU-Standardvertragsklauseln / Data Privacy Framework.
Microsoft Ireland Operations Ltd. One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	E-Mail-Kommunikation mit Bewerbern (Outlook) sowie Ablage und Speicherung von Bewerberunterlagen (OneDrive).	Name, E-Mail-Adresse, Telefonnummer, Mailinhalte, Lebenslauf und Bewerbungsunterlagen	EU Data Boundary (EU/EWR); vereinzelte Support-Zugriffe aus Drittländern möglich. EU-Standardvertragsklauseln / Data Privacy Framework.
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Irland	Ablage und Speicherung von Bewerberunterlagen (insbesondere Lebensläufe), die automatisiert übertragen werden.	Name, Lebenslauf und Bewerbungsunterlagen	Vertragspartner EU (Irland); Drittlandtransfer in die USA möglich. EU-Standardvertragsklauseln / Data Privacy Framework.

Aircall SAS 11-15 rue Saint-Georges, 75009 Paris, Frankreich (Entity gemäß AVV prüfen, ggf. Aircall, Inc., USA)	Telefonie für die Kontaktaufnahme und Vorqualifizierung von Bewerbern (Cloud-Telefonanlage).	Name, Telefonnummer, Gesprächs- und Verbindungsdaten	Vertragspartner EU (Frankreich); je nach Entity Drittlandtransfer möglich. EU-Standardvertragsklauseln.

Hinweis: Nicht in dieser Anlage aufgeführte Dienstleister (insbesondere Vertriebs- und Buchhaltungssoftware sowie Werbeplattformen) verarbeiten keine Bewerberdaten im Auftrag des Auftraggebers und sind daher keine Subunternehmer im Sinne dieses Vertrags.

Anlage 3: Beschreibung der Verarbeitung

Diese Anlage konkretisiert die Angaben aus § 2 und § 3 dieses Vertrags. Für individuelle Angaben (Anschrift des Auftraggebers, Datum und Bezeichnung des Hauptvertrags) ist der Hauptvertrag maßgeblich.

Gegenstand des Auftrags	Verarbeitung personenbezogener Daten im Rahmen der Generierung und Vorqualifizierung von Bewerbungen für den Auftraggeber über Social-Media-Werbeanzeigen. Der Gegenstand ergibt sich im Einzelnen aus dem Hauptvertrag.
Art der Verarbeitung	Erheben, Erfassen, Organisieren, Speichern, Verwenden sowie Übermitteln an den Auftraggeber.
Zweck der Verarbeitung	Generierung von Bewerbungen für den Auftraggeber durch Social-Media-Werbeanzeigen sowie Vorqualifizierung und Bereitstellung der Bewerberdaten an den Auftraggeber.
Kategorien betroffener Personen	Interessenten und Bewerber des Auftraggebers.
Kategorien personenbezogener Daten	Personenstammdaten, Kommunikationsdaten sowie Bewerbungs- und Qualifikationsdaten (z. B. Lebenslauf, Zeugnisse, optionales Bewerbungsfoto). Besondere Kategorien nach Art. 9 DSGVO werden nicht aktiv erhoben.
Dauer der Verarbeitung	Richtet sich nach dem Hauptvertrag und endet bei unbestimmter Laufzeit durch Kündigung des Haupt- oder dieses Vertrags. Nach Beendigung werden die Daten gemäß § 11 zurückgegeben oder gelöscht.