

Anlage Auftragsverarbeitungsvertrag (AVV)

Stand 01.09.2026

1. Gegenstand der Beauftragung

- 1) Der Auftraggeber lässt durch den Auftragnehmer auf Grundlage des Vertrages, zu dem dieser Auftragsverarbeitungsvertrag Anlage ist, personenbezogene Daten im Auftrag verarbeiten. Dieser Auftragsverarbeitungsvertrag geht im Fall von Widersprüchen dem Hauptvertrag vor.
- 2) Ziel der Verarbeitung personenbezogener Daten durch den Auftragnehmer ist die Erbringung der im Hauptvertrag vereinbarten Leistungen. Die Kategorien der von der Verarbeitung Betroffenen und personenbezogenen Daten sind in der Anlage 1 wiedergegeben.

2. Ort der Auftragsverarbeitung

- 1) Die Auftragsverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern nicht anders mit dem Auftraggeber vereinbart.
- 2) Jede Verlagerung der Auftragsverarbeitung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

3. Verantwortlichkeit und Weisungsrecht des Auftraggebers

- 1) Der Auftraggeber ist für die Zwecke der Auftragsverarbeitung der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Übermittlung der Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung durch diesen, verantwortlich.
- 2) Der Auftraggeber hat jederzeit das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Verarbeitung der personenbezogenen Daten zu erteilen. Weisungen können mündlich oder in Textform erfolgen. Mündliche Weisungen des Auftraggebers sind durch diesen unverzüglich in Textform zu bestätigen.
- 3) Der Auftragnehmer wird den Auftraggeber unverzüglich in Textform informieren, wenn nach seiner Auffassung eine vom Auftraggeber erteilte Weisung gegen gesetzliche Regelungen verstößt. Solange die Parteien die Bedenken des

Auftragnehmers nicht ausgeräumt haben, ist der Auftragnehmer berechtigt, die Durchführung der betreffenden Weisung auszusetzen.

4) Sofern der Auftragnehmer der Auffassung sein sollte, eine Weisung des Auftraggebers aus technischen Gründen nicht befolgen zu können, wird er den Auftraggeber hierüber in Textform informieren und sich zum weiteren Vorgehen mit diesem abstimmen.

4. Pflichten des Auftragnehmers

1) Jegliche Verarbeitung der personenbezogenen Daten erfolgt ausschließlich entsprechend den Vorgaben des Hauptvertrages sowie den ggf. vom Auftraggeber erteilten Weisungen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Dieser Absatz 1 gilt nicht, wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2) Der Auftragnehmer bestätigt, dass er gesetzlich nicht verpflichtet ist, einen betrieblichen Datenschutzbeauftragten zu bestellen.

3) Der Auftragnehmer hat die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Umfang der Verpflichtung hat in einem angemessenen Verhältnis zu den verarbeiteten Daten und den Folgen einer etwaigen Verletzung des Schutzes der personenbezogenen Daten zu stehen. Sie hat sich ferner auf alle personenbezogenen Daten zu beziehen, die der Auftragnehmer für den Auftraggeber verarbeitet. Der Inhalt und die Tatsache der Verpflichtung ist dem Auftraggeber auf Wunsch nachzuweisen. Etwaige weitergehende Verpflichtungen, die aus einer gesondert zwischen den Parteien abgeschlossenen Geheimhaltungsvereinbarung folgen, bleiben hiervon unberührt.

4) Der Auftragnehmer darf die für den Auftraggeber verarbeiteten personenbezogenen Daten nicht zu eigenen Zwecken, insbesondere nicht zu Test- oder Trainingszwecken, verarbeiten.

5) Der Auftragnehmer hat sein Verzeichnisse der Auftragsverarbeitung für den Auftraggeber auf Wunsch zu überlassen. Er hat ihn über spätere Änderungen unaufgefordert in Textform zu informieren.

6) Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen. Hierfür wird er insbesondere die in diesem Vertrag vorgesehenen Leistungen erbringen.

7) Der Auftragnehmer wird den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen. Für Unterstützungsleistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu. Er darf die Erbringung der von ihm nach den Vorgaben der DSGVO geschuldeten Leistungen nicht davon abhängig machen, dass die Parteien sich auf ein bestimmtes Entgelt geeinigt haben oder dieses bereits entrichtet wurde.

8) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder ist es zu entsprechenden Maßnahmen gekommen, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber umfassend zu informieren, es sei denn, dies ist ihm gesetzlich nicht gestattet. Ferner ist der Auftragnehmer verpflichtet, alle insoweit relevanten Dritten darauf hinweisen, dass es sich bei den Daten um personenbezogene Daten handelt, für die der Auftraggeber Verantwortlicher ist und er selbst nur als Auftragsverarbeiter tätig wird.

5. Pflichten des Auftraggebers

1) Der Auftraggeber hat den Auftragnehmer unverzüglich unter Angabe der Gründe zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten feststellt.

6. Sicherheit der Verarbeitung

1) Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, insbesondere geeignete technische und organisatorische Maßnahmen, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Zum Zeitpunkt des Vertragsschlusses sind dies die in der Anlage 2 beschriebenen Maßnahmen. Er hat die Einhaltung dieser Vorgaben dem Auftraggeber auf dessen Verlangen mit geeigneten Mitteln nachzuweisen.

2) Der Auftragnehmer ist zur Anpassung an geänderte technische oder rechtliche Gegebenheiten berechtigt, Änderungen an den in Anlage 2 beschriebenen Maßnahmen vorzunehmen. Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen, eine Erhöhung der

Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen oder generell eine Reduktion des vereinbarten Schutzniveaus mit sich bringen könnten, bedürfen der Zustimmung des Auftraggebers. Andere Änderungen, insbesondere eine Verbesserung der ergriffenen Maßnahmen, können vom Auftragnehmer ohne Zustimmung des Auftraggebers umgesetzt werden. Nach Vornahme solcher Änderungen passt der Auftragnehmer die Anlage 2 entsprechend an und übermittelt die jeweils aktuelle Version der Anlage 2 unverzüglich dem Auftraggeber bzw. weist diesen darauf hin, wo die neue Version auf der Webseite des Auftragnehmers zur Verfügung gestellt wird.

7. Betroffenenrechte

1) Der Auftragnehmer wird, soweit es ihm möglich und zumutbar ist, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Personen nachzukommen. Hierfür hat der Auftraggeber den Auftragnehmer in Textform zu informieren, welche Unterstützungshandlung des Auftragnehmers er benötigt und diesem insoweit die Daten zu überlassen, die zur Erfüllung der Anfrage erforderlich sind. Soweit eine Partei weitere Informationen von der anderen Partei benötigt, wird sie diese unverzüglich in Textform darauf hinweisen. Der Auftragnehmer erbringt seine Unterstützungshandlung in angemessener Frist, so dass der Auftraggeber die ihm obliegenden Fristen wahren kann. Er hat den Auftraggeber unverzüglich unter Angabe der Gründe zu informieren, wenn er sich nicht in der Lage sieht, die verlangte Unterstützungshandlung zu erbringen.

2) Wenn ein Betroffener sich zur Ausübung der diesem aus Kapitel 3 der DSGVO zustehenden Rechte unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer diesen an den Auftraggeber verweisen, soweit ihm die Zuordnung zu diesem möglich ist. Sollte ihm eine Zuordnung nicht möglich und der Auftragnehmer auch nicht als Verantwortlicher unmittelbar gegenüber dem Betroffenen aus Kapitel 3 der DSGVO verpflichtet sein, wird er ihn darüber informieren, dass er als Auftragsverarbeiter für Dritte tätig ist und er den Dritten hinsichtlich des Betroffenen nicht identifizieren kann. Sofern und soweit der Auftragnehmer gegenüber dem Betroffenen selbst als Verantwortlicher nach Kapitel 3 der DSGVO verpflichtet ist, obliegt die Erfüllung der entsprechenden Verpflichtungen alleine dem Auftragnehmer als Verantwortlichen.

3) Für Leistungen unter dieser Ziffer steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu. Er darf die Erbringung der

von ihm nach den Vorgaben der DSGVO geschuldeten Leistungen nicht davon abhängig machen, dass die Parteien sich auf ein bestimmtes Entgelt geeinigt haben oder dieses bereits entrichtet wurde.

8. Kontrollrechte des Auftraggebers

1) Dem Auftraggeber stehen alle Kontrollrechte, insbesondere Inspektionen, zu, die zur Wahrung der ihm nach den Vorgaben der DSGVO obliegenden Pflichten erforderlich sind. Das Kontrollrecht ist mit einer angemessenen Ankündigungsfrist und zu den üblichen Geschäftszeiten des Auftragnehmers auszuüben. Der Auftragnehmer ist zur Reduktion der Auswirkungen von Inspektionen auf seinen Geschäftsbetrieb berechtigt, diese mit denen anderer Auftraggeber zu verbinden, soweit dies dem Auftraggeber zumutbar ist (z.B. gemeinsame Inspektionstermine, die in angemessener Frist durchgeführt werden). Der Auftraggeber wird Sorge dafür tragen, dass Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig zu stören.

2) Der Auftraggeber ist berechtigt, die Ausübung der Kontrollrechte auf einem von diesem beauftragten Dritten zu übertragen. Sollte der Dritte in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat dieser gegen dessen Tätigkeit ein Einspruchsrecht.

3) Diese Rechte des Auftraggebers können auch durch Vertragspartner des Auftraggebers ausgeübt werden, wenn und soweit der Auftraggeber für diese personenbezogene Daten im Auftrag verarbeitet und den Auftragnehmer hierfür im Unterauftrag einsetzt.

4) Der Auftragnehmer hat an der Ausübung der Kontrollrechte im erforderlichen Umfang mitzuwirken. Er darf Kontrollen durch den Auftraggeber von der Unterzeichnung einer üblichen und angemessenen Verschwiegenheitserklärung abhängig machen, soweit dies zum Schutz seiner Geschäftsgeheimnisse nach den gesetzlichen Vorgaben erforderlich ist.

5) Für Leistungen unter dieser Ziffer steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu. Er darf die Erbringung der von ihm nach den Vorgaben der DSGVO geschuldeten Leistungen nicht davon abhängig machen, dass die Parteien sich auf ein bestimmtes Entgelt geeinigt haben oder dieses bereits entrichtet wurde.

9. Maßnahmen von Aufsichtsbehörden

1) Der Auftragnehmer informiert, soweit zulässig, den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer (Aufsichts-)Behörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt insbesondere, soweit eine Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Auftragsverarbeitung beim Auftragnehmer ermittelt.

2) Soweit der Auftraggeber seinerseits einer Kontrolle der (Aufsichts-)Behörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer im erforderlichen Umfang zu unterstützen. Für die insoweit zu erbringenden Leistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu, sofern und soweit er die entsprechende Kontrolle etc. nicht zu vertreten hat. Der Auftragnehmer darf die Erbringung der von ihm geschuldeten Leistungen nicht davon abhängig machen, dass der Auftraggeber eine bestimmte Vergütung anerkennt und/oder vorab leistet.

10. Unterauftragsverarbeiter

1) Der Auftragnehmer setzt für die Verarbeitung die in der Anlage 3 benannten Unterauftragsverarbeiter ein.

2) Der Auftragnehmer wird den Auftraggeber in Textform über Änderungen an der Beauftragung von Unterauftragsverarbeitern informieren. Zu diesem Zweck wird der Auftragnehmer dem Auftraggeber in Textform folgende Informationen übersenden:

- a. Beschreibung der geplanten Änderung;
- b. Name und Adresse des Unterauftragsverarbeiters;
- c. welche Leistungen der Unterauftragsverarbeiter erbringen soll und welche personenbezogenen Daten und welche Kategorie von Betroffenen hiervon betroffen sind;
- d. den Inhalt der entsprechenden Vereinbarungen mit dem Unterauftragsverarbeiter sowie ggf. alle Nachweise zur Einhaltung des Kapitels 5 der DSGVO;
- e. die vorstehenden Informationen sind ebenfalls für alle weiteren Unterauftragsverarbeiter zur Verfügung zu stellen, die unterhalb des Unterauftragsverarbeiters entsprechende Leistungen erbringen sollen;

3) Der Auftraggeber kann innerhalb einer Frist von zwei Wochen seit Zugang der Information der Änderung widersprechen. Der Auftragnehmer setzt die Änderung nicht vor Ablauf der Widerspruchsfrist um. Im Falle eines Widerspruchs ist der Auftragnehmer berechtigt, den Auftragsverarbeitungsvertrag mit einer Frist von mindestens einem Monat zu kündigen, sofern die Änderung dem Auftraggeber zumutbar gewesen wäre und der Widerspruch dem Auftragnehmer unzumutbar ist. Zumutbarkeit für den Auftraggeber ist gegeben, wenn mit der Änderung keine Nachteile für ihn zu befürchten gewesen wären und insbesondere sichergestellt gewesen wäre, dass die Vorgaben dieses Vertrages und der DSGVO bei Umsetzung der Änderung weiter eingehalten worden wären. Unzumutbarkeit für den Auftragnehmer ist gegeben, wenn er seine Auftragsverarbeitungsleistungen als im Wesentlichen gleichförmigen Prozess für eine Vielzahl von Auftraggebern erbringt und individuelle Abweichungen bei den Unterauftragsverarbeitern für den Auftragnehmer nicht einfach umzusetzen sind (z.B. alle Auftraggeber nutzen dieselbe, standardisierte Softwareplattform).

4) Der Auftragnehmer wird für eventuelle Unterauftragsverarbeiter die in den Absätzen 2 und 4 des Art. 28 DSGVO genannten Bedingungen einhalten. Er hat ferner sicherzustellen, dass die sonst mit dem Auftraggeber insoweit getroffenen vertraglichen Vereinbarungen sowie die ggf. ergänzende Weisungen des Auftraggebers auch von den Auftragsverarbeitern eingehalten werden. Er hat dies dem Auftraggeber auf dessen Wunsch nachzuweisen.

11. Verstoß gegen datenschutzrechtliche Vorschriften

1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die getroffenen Vereinbarungen und/oder die erteilten Weisungen unverzüglich, spätestens 24 Stunden nach erster Kenntnis, in Textform mitzuteilen.

2) Jegliche, etwaige erforderliche Meldung an eine Aufsichtsbehörde oder Information von Betroffenen obliegt allein dem Auftraggeber. Der Auftragnehmer wird hieran im erforderlichen Umfang mitwirken.

3) Der Auftragnehmer ist weiter verpflichtet, den Verstoß im erforderlichen Umfang unverzüglich aufzuklären und dem Auftraggeber eine entsprechende Dokumentation zu überlassen. Die Dokumentation hat eine Darstellung zu umfassen, welche Maßnahmen der Auftragnehmer ergriffen hat, um weitere Verstöße zu unterbinden und warum er der Auffassung ist, dass die ergriffenen Maßnahmen ausreichend sind, um den Vorgaben dieses Vertrages und der gesetzlichen Vorschriften zu genügen.

12. Vergütung des Auftragnehmers

1) Dem Auftragnehmer steht für die von ihm unter diesem Vertrag erbrachten Leistungen kein gesondertes Entgelt zu, sofern nicht anders in diesem Vertrag vereinbart.

13. Haftung

1) Die Haftung der Parteien richtet sich nach den Vereinbarungen des Hauptvertrages.

14. Dauer des Vertrages

1) Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

15. Folgen der Vertragsbeendigung

1) Der Auftragnehmer wird nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder einem strukturierten, gängigen und maschinenlesbaren Format zurückgeben und die vorhandenen Kopien löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Auftragnehmer unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftragnehmer hat die Durchführung der Löschung entsprechend den Vorgaben des Auftraggebers diesem zu bestätigen.

2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren.

3) Jegliches Zurückbehaltungsrecht Auftragnehmers hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ist im Übrigen ausgeschlossen.

16. Schlussbestimmungen

1) Es gelten die Schlussbestimmungen des Hauptvertrages.

Anlage 1 – Kategorien personenbezogener Daten und betroffener Personen

Kategorien personenbezogener Daten:

Kandidatendaten samt Bewerbungsunterlagen (insb. Name, Adresse, Kontaktdaten, Lebenslauf, Zeugnisse)

Kategorien der von der Auftragsverarbeitung Betroffenen:

Kandidaten für eine ausgeschriebene Stelle

Anlage TOM – Technische und organisatorische Maßnahmen (AVV-Anlage 2)

17. Zuordnung zu klassischen Kontrollbereichen

- 1) Klassische Kategorie | Entsprechende Abschnitte dieser Anlage
- 2) Zutrittskontrolle | 2.3
- 3) Zugangskontrolle | 2.4
- 4) Zugriffskontrolle | 2.5
- 5) Weitergabekontrolle | 2.7
- 6) Eingabekontrolle | 2.8
- 7) Auftragskontrolle / Weisungskontrolle | 2.1, 2.6, 2.14
- 8) Verfügbarkeitskontrolle | 2.9
- 9) Trennungskontrolle | 2.6
- 10) Löschung / Vernichtung | 2.12
- 11) Datenschutz durch Technikgestaltung / Voreinstellungen | 2.11

18. Beschreibung der TOMs

- 1) Organisation, Governance und Weisungsmanagement
 - a) Es bestehen dokumentierte Richtlinien bzw. verbindliche Vorgaben zu Datenschutz, Informationssicherheit, Berechtigungsmanagement, Passwort-/Authentisierungsvorgaben, Verschlüsselung, Umgang mit Sicherheitsvorfällen, Backup/Restore, Löschung, Remote Work, Change-/Release-Management und Lieferantenmanagement.
 - b) Zuständigkeiten und Eskalationswege für Datenschutz, Informationssicherheit, Incident Response und operative Umsetzung sind intern festgelegt.
 - c) Weisungen des Verantwortlichen werden dokumentiert und den jeweils zuständigen Stellen zugänglich gemacht.
 - d) Zugriffe auf personenbezogene Daten zu Support-, Wartungs- oder Analysezwecken erfolgen nur auf dokumentierter Grundlage und im erforderlichen Umfang.

- e) Abweichungen von internen Sicherheitsvorgaben oder Freigaben von Ausnahmen werden dokumentiert, bewertet und genehmigt.
- f) Sicherheits- und Datenschutzanforderungen werden bei wesentlichen Änderungen von Prozessen, Systemen oder Subdienstleistern überprüft.
- 2) Personal, Vertraulichkeit und Awareness
 - a) Mitarbeitende sowie eingesetzte Dritte werden vor Aufnahme ihrer Tätigkeit auf Vertraulichkeit verpflichtet.
 - b) Rollen und Verantwortlichkeiten werden im Rahmen von Onboarding, Rollenwechsel und Offboarding definiert und dokumentiert.
 - c) Mitarbeitende werden regelmäßig zu Datenschutz, Informationssicherheit, Phishing-/Social-Engineering-Risiken und Meldewegen für Sicherheitsvorfälle geschult.
 - d) Der Zugang zu personenbezogenen Daten wird nur solchen Personen eingeräumt, die ihn für ihre Aufgabenerfüllung benötigen.
 - e) Beim Ausscheiden oder Rollenwechsel werden Berechtigungen unverzüglich angepasst bzw. entzogen und dienstliche Assets zurückgegeben.
 - f) Soweit rechtlich zulässig und nach Risikolage angezeigt, werden zusätzliche personelle Sicherheitsmaßnahmen eingesetzt (z. B. Referenzprüfungen, erweiterte Freigabeprozesse für privilegierte Rollen).
- 3) Zutrittskontrolle (physische Sicherheit)
 - a) Büro-, Technik- und sonstige sensible Bereiche sind gegen unbefugten Zutritt geschützt, etwa durch Schließsysteme, Zugangskarten, Schlüsselverwaltung, Empfangs- oder Besucherkonzepte.
 - b) Besucher erhalten nur begleitet oder kontrolliert Zugang; Besuche können dokumentiert werden.
 - c) Server- und Netzwerkinfrastruktur in eigenen Räumen wird in besonders geschützten Bereichen betrieben.
 - d) Papierunterlagen und Datenträger mit personenbezogenen Daten werden vor unbefugtem Zugriff geschützt aufbewahrt.
 - e) Nicht mehr benötigte Papierunterlagen und physische Datenträger werden datenschutzgerecht vernichtet bzw. entsorgt.

f) Soweit Rechenzentrumsleistungen durch Cloud- oder Hosting-Anbieter erbracht werden, werden deren physische Sicherheitsmaßnahmen vertraglich abgesichert und anhand geeigneter Nachweise überprüft.

4) Zugangskontrolle (Authentisierung)

a) Für den Zugang zu IT-Systemen werden grundsätzlich individuelle Benutzerkennungen verwendet.

b) Gemeinsame Benutzerkonten werden nur in begründeten Ausnahmefällen für technisch notwendige Service-Accounts eingesetzt; deren Nutzung ist gesondert abgesichert und dokumentiert.

c) Authentisierung erfolgt mittels starker Passwörter, Single-Sign-On, passwortlosen Verfahren oder vergleichbaren sicheren Verfahren.

d) Multifaktor-Authentisierung wird insbesondere für privilegierte Zugänge, Administrationszugänge, Remote-Zugänge und produktionsnahe Systeme eingesetzt.

e) Sitzungen werden angemessen zeitlich begrenzt; automatische Sperren bzw. Re-Authentisierungen sind vorgesehen.

f) Notfall- oder Break-Glass-Zugänge sind besonders geschützt, begrenzt und überwacht.

5) Zugriffskontrolle (Berechtigungen)

a) Es besteht ein dokumentiertes Rollen- und Berechtigungskonzept.

b) Rechte werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben.

c) Berechtigungen werden nur auf Antrag bzw. im Rahmen definierter Prozesse vergeben, geändert und entzogen.

d) Berechtigungen werden regelmäßig sowie anlassbezogen überprüft.

e) Administrationsrechte sind auf einen engen Personenkreis beschränkt und von normalen Benutzerkonten getrennt.

f) Zugriffe auf besonders schutzbedürftige Daten, produktive Datenbanken, Exportfunktionen, Administrationsoberflächen oder Quellcode-Repositories sind gesondert geregelt und protokolliert.

6) Trennungskontrolle / Mandantentrennung / Umgebungs-Trennung

a) Daten verschiedener Verantwortlicher bzw. Mandanten werden logisch voneinander getrennt verarbeitet.

- b) Mandanten-, Kunden-, Projekt- oder Workspace-Strukturen verhindern eine ungewollte Vermischung von Datenbeständen.
 - c) Entwicklungs-, Test-, Staging- und Produktivumgebungen sind voneinander getrennt.
 - d) Produktivdaten werden in Test- oder Entwicklungsumgebungen nur verwendet, wenn dies erforderlich ist und zusätzliche Schutzmaßnahmen bestehen (z. B. Pseudonymisierung, Maskierung, reduzierte Datensätze, gesonderte Freigabe).
 - e) Schlüssel, Secrets, Zugangsdaten und Rollen werden umgebungsbezogen getrennt verwaltet.
 - f) Bei Agenturleistungen werden Kundenkonten, Kampagnenzugänge, Zielgruppenlisten und Reportings mandantenbezogen getrennt geführt.
- 7) Weitergabekontrolle / Übermittlung / Transport / Schnittstellen
- a) Personenbezogene Daten werden bei der Übertragung über öffentliche oder ungesicherte Netze dem Stand der Technik entsprechend geschützt (z. B. Transportverschlüsselung).
 - b) Fernzugriffe auf interne Systeme erfolgen nur über gesicherte Verbindungen und definierte Zugangskanäle.
 - c) API-, Import-, Export- und Integrationsschnittstellen sind authentisiert, rollenbasiert abgesichert und möglichst auf erforderliche Berechtigungen bzw. Scopes beschränkt.
 - d) Datenexporte, Massenabfragen oder Datenweitergaben können funktional beschränkt, freigabepflichtig oder protokolliert sein.
 - e) E-Mail-, Datei- oder Datenaustauschprozesse sind so ausgestaltet, dass Fehlversendungen und unbefugte Offenlegungen reduziert werden.
 - f) Externe Empfänger, Unterauftragnehmer oder sonstige Empfängerkreise werden vor einer Weitergabe anhand definierter Prozesse geprüft.
 - g) Soweit Daten an Dritte oder in Drittländer übermittelt werden, erfolgt dies nur auf dokumentierter Grundlage und unter Beachtung der hierfür vorgesehenen vertraglichen und gesetzlichen Anforderungen.
- 8) Eingabekontrolle / Protokollierung / Nachvollziehbarkeit
- a) Relevante Systemereignisse werden protokolliert, insbesondere Anmeldungen, fehlgeschlagene Anmeldeversuche, Berechtigungsänderungen, Administratorhandlungen, sicherheitsrelevante Konfigurationsänderungen und –

soweit angemessen – Datenexporte, Löschungen oder sonstige kritische Verarbeitungsvorgänge.

b) Protokolle werden gegen unbefugten Zugriff und unbefugte Veränderung geschützt.

c) Zugriffe auf Protokolle sind auf einen berechtigten Personenkreis beschränkt.

d) Für sicherheitsrelevante Systeme bestehen Monitoring- und Alarmierungsmechanismen.

e) Zeitquellen und Uhrzeitsynchronisation der Systeme werden konsistent gehalten, um eine belastbare Nachvollziehbarkeit zu ermöglichen.

f) Aufbewahrungsfristen für Protokolle werden festgelegt und an Zweck, Schutzbedarf und rechtliche Anforderungen angepasst.

9) Verfügbarkeitskontrolle / Resilienz / Wiederherstellbarkeit

a) Es besteht ein dokumentiertes Backup- und Wiederherstellungskonzept.

b) Datensicherungen werden regelmäßig erstellt, gegen unbefugten Zugriff geschützt und getrennt vom Produktivbetrieb aufbewahrt.

c) Wiederherstellungsverfahren werden regelmäßig überprüft oder getestet.

d) Verfügbarkeit, Kapazitäten und wesentliche Systemzustände werden überwacht.

e) Für kritische Systeme bestehen Maßnahmen zur Redundanz, Ausfallsicherheit oder Notfallüberbrückung, soweit dies nach Risikolage oder Leistungsversprechen erforderlich ist.

f) Notfall- und Wiederanlaufprozesse sind dokumentiert; Zuständigkeiten und Kommunikationswege sind definiert.

g) Soweit relevant, werden Zielgrößen für Wiederanlauf und Datenwiederherstellung (z. B. RTO/RPO) festgelegt oder vertraglich beschrieben.

10) Integrität, Betriebs- und Änderungssicherheit

a) Für produktive Systeme bestehen geregelte Prozesse für Änderungs-, Release- und Patch-Management.

b) Sicherheitsrelevante Updates und Patches werden risikoorientiert bewertet, priorisiert und eingespielt.

c) Systeme werden gehärtet und anhand definierter Baselines oder Standardkonfigurationen betrieben, soweit dies möglich ist.

- d) Es bestehen Prozesse für Schwachstellenmanagement, inklusive Identifikation, Bewertung, Priorisierung und Behebung von Schwachstellen.
- e) Soweit nach Risikolage angezeigt, werden technische Prüfungen wie Security-Tests, externe Assessments oder Penetrationstests durchgeführt.
- f) Fehler- und Störungsbehebungen werden dokumentiert und mit Incident- bzw. Change-Prozessen verzahnt.
- g) Schadsoftware-Schutz, EDR/AV oder vergleichbare Schutzmechanismen werden eingesetzt, soweit dies für die betroffenen Systeme angemessen ist.
- 11) Verschlüsselung, Pseudonymisierung und Datenschutz durch Technikgestaltung / Voreinstellungen
 - a) Daten werden bei Übertragung und – soweit nach Risikolage angezeigt – auch bei Speicherung verschlüsselt.
 - b) Mobile Endgeräte und Datenträger mit personenbezogenen Daten sind, soweit eingesetzt, angemessen verschlüsselt.
 - c) Kryptografische Schlüssel und sonstige Geheimnisse werden kontrolliert verwaltet; Klartextspeicherung in Quellcode, Tickets oder ungesicherten Ablagen wird vermieden.
 - d) Pseudonymisierung, Maskierung, Kürzung oder Aggregation von Daten werden eingesetzt, soweit dies mit dem Verarbeitungszweck vereinbar ist.
 - e) Systeme und Prozesse sind so gestaltet, dass standardmäßig nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten verarbeitet werden.
 - f) Standard- und Grundeinstellungen werden möglichst datenschutzfreundlich gewählt (z. B. restriktive Freigaben, begrenzte Sichtbarkeiten, kurze Standard-Aufbewahrungen, deaktivierte unnötige Tracking- oder Exportfunktionen).
 - g) Neue oder wesentlich geänderte Funktionen werden im Hinblick auf Datenschutz- und Sicherheitsanforderungen überprüft.
- 12) Löschung, Sperrung, Rückgabe und Vernichtung
 - a) Es besteht ein Lösch- bzw. Aufbewahrungskonzept mit definierten Fristen, Verantwortlichkeiten und Prozessen.
 - b) Personenbezogene Daten werden nach Zweckwegfall, Vertragsende oder entsprechender Weisung gelöscht, gesperrt oder zurückgegeben, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

- c) Rückgaben bzw. Exporte an den Verantwortlichen erfolgen in einem gängigen, strukturierten Format, soweit dies vertraglich vorgesehen ist.
- d) Löschungen in Produktivsystemen, Backups, Archivsystemen und bei Unterauftragnehmern werden prozessual berücksichtigt.
- e) Datenträger und Hardware werden vor Aussonderung datenschutzgerecht gelöscht oder vernichtet.
- f) Support-, Ticket-, Protokoll- und Exportdaten werden in das Löschkonzept einbezogen, soweit sie personenbezogene Daten enthalten.

13) Incident Response und Umgang mit Datenschutzverletzungen

- a) Es besteht ein dokumentierter Prozess für das Erkennen, Bewerten, Eindämmen, Beheben und Nachbereiten von Sicherheitsvorfällen und Datenschutzverletzungen.
- b) Sicherheitsereignisse werden nach Schweregrad klassifiziert und an definierte Stellen eskaliert.
- c) Mitarbeitende kennen Meldewege für Sicherheitsvorfälle und Datenschutzverletzungen.
- d) Der Verantwortliche wird über Datenschutzverletzungen unverzüglich nach Kenntniserlangung informiert; die Meldung enthält, soweit verfügbar, die zur rechtlichen Bewertung und weiteren Maßnahmen erforderlichen Informationen.
- e) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Aufklärung, Eindämmung, Dokumentation und Erfüllung gesetzlicher Melde- bzw. Benachrichtigungspflichten.
- f) Maßnahmen zur Ursachenanalyse, Beweissicherung und Lessons Learned sind vorgesehen.

14) Unterauftragsverarbeiter und Lieferantenmanagement

- a) Unterauftragsverarbeiter und sicherheitsrelevante Lieferanten werden anhand definierter Auswahl- und Prüfprozesse bewertet.
- b) Mit Unterauftragsverarbeitern werden vertragliche Vereinbarungen geschlossen, die ein angemessenes Sicherheits- und Datenschutzniveau sicherstellen.
- c) Eine aktuelle Liste der Unterauftragsverarbeiter wird geführt; Änderungen werden nach den vertraglichen Vorgaben mitgeteilt.

d) Sicherheits- und Datenschutznachweise von Unterauftragnehmern werden risikoorientiert angefordert, geprüft oder ausgewertet (z. B. Audits, Berichte, Zertifikate, Selbstauskünfte).

e) Soweit Cloud-Infrastruktur Dritter genutzt wird, werden Verantwortlichkeiten entlang des Shared-Responsibility-Modells intern und vertraglich klar zugeordnet.

f) Internationale Datenflüsse und Zugriffe durch Unterauftragnehmer werden gesondert bewertet und dokumentiert.

15) Mobile Arbeit, Homeoffice und Endgerätesicherheit

a) Mobile Arbeit und Homeoffice unterliegen verbindlichen Vorgaben.

b) Zugriffe auf personenbezogene Daten erfolgen grundsätzlich nur über freigegebene, angemessen abgesicherte Endgeräte oder in ausdrücklich geregelten Ausnahmefällen unter zusätzlichen Schutzmaßnahmen.

c) Endgeräte werden mit Bildschirmsperre, Festplattenverschlüsselung, aktuellem Patchstand und angemessenem Endpoint-Schutz betrieben.

d) Lokale Administratorrechte sind, soweit möglich, beschränkt.

e) Der Zugriff von unterwegs erfolgt über gesicherte Verbindungen und mit starker Authentisierung.

f) Verlust, Diebstahl oder Kompromittierung von Endgeräten sind unverzüglich zu melden; Fernsperrung oder Fernlöschung ist, soweit technisch möglich, vorgesehen.

16) Entwicklungsprozesse / DevSecOps / Produkt- und Service-Sicherheit

a) Für Eigenentwicklungen bestehen definierte Entwicklungs- und Freigabeprozesse.

b) Quellcode, Repositories, CI/CD-Pipelines und Build-Artefakte sind gegen unbefugten Zugriff geschützt.

c) Änderungen werden vor Produktivsetzung getestet und freigegeben.

d) Sicherheits- und Datenschutzanforderungen werden im Entwicklungsprozess berücksichtigt (z. B. Code-Review, Secret-Management, Dependency-Management, abgesicherte Standardkonfigurationen).

e) Produktive Zugangsdaten und Secrets werden nicht ungeschützt in Quellcode oder sonstigen ungesicherten Ablagen gespeichert.

f) Soweit relevant, bestehen Verfahren für sichere Rücknahme von Releases und für die Behandlung sicherheitsrelevanter Findings.

- 17) Branchenspezifische Ergänzungen für SaaS / Cloud / digitale Dienste
- a) Die Leistung ist mandantenfähig oder vergleichbar getrennt ausgestaltet; Mandanten können nur auf ihre jeweils zugeordneten Daten zugreifen.
 - b) Kundenadministratoren erhalten rollenbasierte Verwaltungsfunktionen; privilegierte Aktionen können protokolliert werden.
 - c) Supportzugriffe auf Kundendaten sind nach Möglichkeit ticketbasiert, zeitlich begrenzt und nachvollziehbar.
 - d) Soweit angeboten, bestehen Funktionen für Export, Berichtigung, Löschung, Rollenverwaltung und Aufbewahrungssteuerung.
 - e) Öffentliche Schnittstellen und Administrationsoberflächen sind angemessen abgesichert; nicht benötigte Dienste und Ports werden deaktiviert oder beschränkt.
 - f) Resilienz- und Sicherheitsmaßnahmen für Internet-exponierte Dienste (z. B. Rate Limiting, WAF, DDoS-Schutz, Monitoring) werden nach Risikolage eingesetzt.
- 18) Branchenspezifische Ergänzungen für Online-Marketing / Agenturen / Kampagnensteuerung
- a) Kundenkonten bei Werbe-, Analyse-, CRM- oder Kommunikationsplattformen werden mandantenbezogen getrennt verwaltet.
 - b) Zugänge zu Kundenplattformen werden nur personenbezogen oder über freigegebene Unternehmenszugänge verwaltet; private oder unkontrollierte Account-Nutzung ist ausgeschlossen oder ausdrücklich untersagt.
 - c) Zielgruppenlisten, Leads, Reportings und Rohdaten werden nur im erforderlichen Umfang verarbeitet und nach Möglichkeit aggregiert oder pseudonymisiert.
 - d) Exporte, Audience-Uploads, Datenabgleiche und Freigaben für Kampagnen mit Personenbezug unterliegen definierten Prozessen; bei erhöhtem Risiko kann ein Vier-Augen-Prinzip vorgesehen sein.
 - e) Kundenbezogene Daten werden nach Projektende, Mandatsende oder Weisung aus Arbeitsumgebungen entfernt bzw. zurückgegeben, soweit keine Aufbewahrungspflichten bestehen.
 - f) Dienstleister- oder Plattformwechsel werden so gestaltet, dass Datenbestände geordnet übertragen, gelöscht oder gesperrt werden können.

19. Zusätzliche Maßnahmen bei erhöhtem Risiko (optional, soweit einschlägig)

1) Bei erhöhtem Risiko, großen Datenmengen, sensiblen Daten, umfangreicher Profilbildung oder besonders kritischen Services gelten ergänzend insbesondere folgende Maßnahmen:

- a) verpflichtende Multifaktor-Authentisierung für alle administrativen und produktionsnahen Zugänge;
- b) Verschlüsselung sensibler Daten auch im Ruhezustand;
- c) engmaschigere Berechtigungs-Reviews und verstärkte Protokollierung privilegierter Aktivitäten;
- d) häufigere Restore-Tests, Notfallübungen und Sicherheitsprüfungen;
- e) zusätzliche Pseudonymisierung bzw. Trennung identifizierender Merkmale;
- f) restriktivere Export- und Freigabeprozesse;
- g) erweiterte Lieferanten- und Drittlandprüfung;
- h) formalisierte Datenschutz- und Sicherheitsprüfung vor Einführung neuer Funktionen oder Tools.

Anlage Unterauftragsverarbeiter (AVV-Anlage 3)

Anbieter / Vertragspartner	Leistung	Betroffene Daten	Verarbeitungsort	Drittlandmechanismus
Base44, Inc. San Francisco, California USA E-Mail: compliance@base44.com	Produktive Simplyfind-App: Plattformbetrieb, Cloudhosting/Laufzeitumgebung, Datenbank und Datenspeicherung, Datei- und Dokumentenspeicherung, Authentifizierungsbasis, internes Logging/Fehleranalyse, technische Sicherheitsüberwachung sowie integrierte KI-Funktionen	Plattform-, Nutzer-, Kandidaten-, Bewerbungs-/Dokument-, Prozess-, Kommunikations- und technische Protokolldaten	USA; bei künftig aktivierter abweichender Datenregion ist der tatsächlich konfigurierte Verarbeitungsort zu dokumentieren	EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914; EU-US Data Privacy Framework, soweit für den jeweiligen Empfänger anwendbar
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Tägliche zusätzliche Datensicherung / Backup-Speicherung für die Wiederherstellung des Simplyfind-Plattformbetriebs	In den Sicherungen enthaltene Plattform-, Nutzer-, Kandidaten-, Bewerbungs-/Dokument-, Prozess- und technische Daten, soweit für die Wiederherstellung erforderlich	EU-Serverstandort; gemäß Hetzner-AVV werden bei gewähltem EU-Serverstandort Serverdaten ausschließlich innerhalb der EU verarbeitet; Support für diese Standorte innerhalb der EU	Kein Drittlandmechanismus erforderlich, solange ausschließlich ein EU-Serverstandort genutzt wird
Brevo Sendinblue 17 rue Salneuve 75017 Paris France RCS Paris 498 019 298 SAS au capital social de 388 177 euros SIRET 498 019 298 00112 FR80498019298 USt.-Nr. : FR80498019298	Transaktionaler E-Mail-Versand und Systembenachrichtigungen	E-Mail-Adresse, Name soweit erforderlich, Template-/Nachrichtenvariablen sowie Zustell-, Bounce- und Versandmetadaten; keine Bewerbungsunterlagen, soweit technisch vermeidbar	Produktive Datenbanken nach Anbieterangaben innerhalb der EU (u. a. OVH Frankreich/Deutschland und Google Cloud Belgien)	Innerhalb EU/EWR kein Drittlandmechanismus erforderlich; etwaige Drittlandtransfers über Brevo-Unterauftragnehmer nur nach Brevo-DPA und Art. 44 ff. DSGVO
Google Workspace Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Irland.	Gmail, Drive/Docs/Sheets, Calendar und Meet für geschäftliche Kommunikation, Zusammenarbeit, Termine sowie Support-/Recruiting-Kommunikation	Geschäftliche Kontakt- und Nutzerdaten, Kommunikationsinhalte, Termin-/Kalenderdaten, Kunden- und Recruiting-Partnerdaten sowie ggf. personenbezogene Support- und Recruitinginformationen;	EU bzw. gemäß aktivierter Google-Workspace-Datenregionsrichtl inie; für unterstützte Dienste soll Europa verwendet werden	Google Cloud Data Processing Addendum; für etwaige Drittlandverarbeitungen die dort vorgesehenen Garantien nach Art. 44 ff. DSGVO, einschließlich SCC bzw.

Anbieter / Vertragspartner	Leistung	Betroffene Daten	Verarbeitungsort	Drittlandmechanismus
		Kandidatenunterlagen nur ausnahmsweise als vorübergehende Arbeitskopie		Angemessenheitsbeschlüssen, soweit anwendbar
updown.io / Adrien Rey-Jarthon (EI), Frankreich	Externe Verfügbarkeits- und Performanceüberwachung definierter Simplyfind-Endpunkte sowie Alarmierung bei Nichterreichbarkeit	Technische Metadaten zu überwachten URLs/Endpoints, Antwortzeiten, Statuscodes und ggf. Empfängerdaten für Alerts; keine gezielte Übermittlung von Kandidaten-, Bewerbungs- oder Plattforminhalten	Frankreich; etwaige weitere Verarbeitungsorte gemäß aktueller updown.io-DPA/Subprozessorenliste	Innerhalb EWR grundsätzlich kein Drittlandmechanismus erforderlich; für etwaige Drittlandtransfers gelten die im updown.io-DPA vorgesehenen Garantien
Anthropic, PBC Sitz: San Francisco, USA · Rechtsgrundlage: EU-Standardvertragsklauseln (EU-Beschluss 2021/914) Google LLC Sitz: Mountain View, USA · Rechtsgrundlage: EU-US Data Privacy Framework, EU-Standardvertragsklauseln OpenAI, L.L.C. Sitz: San Francisco, USA · Rechtsgrundlage: EU-Standardvertragsklauseln (EU-Beschluss 2021/914)	KI-/LLM- und sonstige technische Funktionen innerhalb der Base44-Leistung	Je nach Funktion minimierte strukturierte Profil-, Dokument-, Matching- oder technische Daten	gemäß jeweils aktueller Base44-Subprozessorenliste	über Base44-DPA/Subprozessorenkette; jeweiliger Transfermechanismus nach aktueller Base44-Dokumentation