

ERNENNUNG ZUM AUFTRAGSVERARBEITER FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN GEMÄSS ART. 28 DSGVO (EU) 2016/679 (GDPR)

zwischen

dem Kunden, wie in den allgemeinen Geschäftsbedingungen des todool-Dienstleistungsvertrages angegeben, nachstehend auch „**Verantwortlicher der Datenverarbeitung**“ oder nur „**Verantwortlicher**“ genannt;

und

todool GmbH mit Sitz in 39052 Kaltern an der Weinstraße (BZ), Sternngasse 6, MwSt-Nr. 03085210213, PEC: todool@pec.it, nachstehend auch „**Auftragsverarbeiter**“ genannt.

Vorbemerkungen und Begriffsbestimmungen

- a) Der Verantwortliche und der Auftragsverarbeiter (beide auch als „**Vertragsparteien**“ bezeichnet) haben einen Dienstleistungsvertrag für die todool-Anwendung abgeschlossen, dessen Ausführung die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen umfasst;
- b) der Auftragsverarbeiter verfügt über genügend Erfahrung, Fähigkeiten und Zuverlässigkeit, um angemessene technische und organisatorische Maßnahmen umzusetzen und die Rolle des Auftragsverarbeiters für die Verarbeitung personenbezogener Daten zu übernehmen;
- c) mit diesem Schreiben beabsichtigen die Parteien, ihre jeweiligen Verpflichtungen im Bereich der Verarbeitung gemäß Buchstabe a) („**Verarbeitung**“) zu regeln, insbesondere durch die Bindung des Auftragsverarbeiters an den Verantwortlichen und die Festlegung von Gegenstand und Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien der betroffenen Personen, Pflichten und Rechte des Verantwortlichen;
- d) wenn im vorliegenden Schreiben Begriffe verwendet werden, denen die Verordnung (EU) 2016/679 („**GDPR**“) eine Definition zuordnet, erhalten diese Begriffe eine solche spezifische Bedeutung, sofern die in diesem Schreiben enthaltenen Angaben die Definitionen im Vertrag nicht verändern oder beeinträchtigen, die daher unverändert bleiben. Für die Zwecke dieses Schreibens wird die benennende Stelle als Verantwortlicher bezeichnet, ungeachtet der Tatsache, dass sie für bestimmte personenbezogene Daten in Bezug auf einen

anderen Verantwortlichen tatsächlich ein Auftragsverarbeiter sein kann. Sofern nicht anders angegeben, bedeuten **„personenbezogene Daten“** bzw. **„betroffene Personen“** die personenbezogenen Daten, die vom Auftragsverarbeiter im Namen des Verantwortlichen verarbeitet werden und die Personen, mit denen diese Daten verbunden sind. Die **„übermittelten Daten“** (und die damit zusammenhängenden Begriffe wie Datenübermittlung usw.) sind personenbezogene Daten, die vom Auftragsverarbeiter im Namen des Verantwortlichen direkt verarbeitet werden, oder die durch Dritte oder Interessierte auf Anweisung des Verantwortlichen dem Auftragsverarbeiter mitgeteilt werden;

- e) dieses Schreiben ergänzt den Vertrag in Bezug auf den Zweck gemäß Punkt c), während der Rest des Inhalts vom Vertrag unverändert bleibt.

Artikel 1 – Bestimmung der Rolle

1.1 – todool GmbH übernimmt die Rolle des Auftragsverarbeiters und ist mit allen – und ausschließlich jenen – Verarbeitungsvorgänge personenbezogener Daten betraut, die zur Ausführung der Vertragsinhalte erforderlich sind. Der Zweck der Verarbeitung steht im Zusammenhang mit der Verwaltung der Steuerpflichten der Subjekte (die somit die betroffenen Personen sind), für die der Verantwortliche die Anwendung todool verwendet. Die verarbeiteten Daten können entweder zur Kategorie der allgemeinen Daten oder zu besonderen Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten) gehören.

1.2 – Die Datenverarbeitungsvorgänge erfolgen mit Hilfe von Datenträgern.

1.3 – Der Auftragsverarbeiter ist verpflichtet, personenbezogene Daten gemäß den Grundsätzen und Bestimmungen des GDPR, dem Gesetz über den Schutz personenbezogener Daten im Allgemeinen und den Verordnungen der zuständigen Aufsichtsbehörde zu verarbeiten, in jedem Fall aber unter Einhaltung der schriftlichen Anweisungen des Verantwortlichen.

1.4 – Der Verantwortliche hält die von der Datenschutz-Grundverordnung festgelegten Verpflichtungen und die ihm von der zuständigen Aufsichtsbehörde auferlegten Bestimmungen ein.

Artikel 2 – Erklärungen und Garantien des Verantwortlichen

2.1 – Der Verantwortliche erklärt, dass die vom Auftragsverarbeiter verarbeiteten Daten relevant sind und den Zweck, für den sie erhoben und anschließend verarbeitet werden, nicht überschreiten, und dass sie gemäß jeder geltenden Vorschrift gesammelt und dann verarbeitet werden. Es wird darauf hingewiesen, dass der

Verantwortliche für die Ermittlung der Rechtsgrundlage für die Verarbeitung personenbezogener Daten verantwortlich ist.

Artikel 3 – Pflichten, Erklärungen und Garantien des Auftragsverarbeiters

3.1 – Unbeschadet des Vorstehenden und der Bestimmungen der folgenden Artikel, verpflichtet sich, erklärt und gewährleistet der Auftragsverarbeiter, dass:

- die zu verarbeitenden personenbezogenen Daten ausschließlich aus den vom Verantwortlichen übermittelten Daten bestehen und der Auftragsverarbeiter keine andere Form des Erwerbs der genannten personenbezogenen Daten verwenden wird;
- für seine eigenen Verpflichtungen personenbezogene Daten gemäß den vom Verantwortlichen festgelegten Zwecken und Methoden verarbeitet werden.

Artikel 4 – Sicherheitsmaßnahmen

4.1 – Der Auftragsverarbeiter ergreift Maßnahmen, um die Sicherheit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten und das Risiko der absichtlichen oder unbeabsichtigten Zerstörung oder des Verlusts von Daten, des unberechtigten Zugriffs, der unbefugten Verarbeitung und der nicht den angegebenen Zwecken entsprechenden Verarbeitung auf ein Mindestmaß zu reduzieren.

4.2 – Der Auftragsverarbeiter verpflichtet sich in jedem Fall, seine Systeme an die technischen und organisatorischen Sicherheitsmaßnahmen anzupassen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, wie gemäß GDPR Art. 32 vorgesehen, sowie ihre Einhaltung regelmäßig zu überprüfen. In jedem Fall sind die folgenden Sicherheitsmaßnahmen einzuhalten:

- in Bezug auf die Vertraulichkeit personenbezogener Daten:
 - a) physischer Schutz der Räumlichkeiten und Geräte, in denen die Verarbeitung stattfindet
 - b) physische und logische Zugangssicherheit
 - c) Zuweisung angemessener Datenzugriffsrechte
 - d) Einsatz von Verschlüsselungstechniken
 - e) sichere Vernichtung von physischen und digitalen Dokumenten
- in Bezug auf die Integrität personenbezogener Daten:
 - a) Schutz der Datenübermittlung
 - b) Sicherheit der Datenverarbeitung
 - c) Schutz von Computersystemen
- in Bezug auf die Verfügbarkeit personenbezogener Daten:

- a) Backup-Maßnahmen
- b) Business continuity-Pläne.

Die vom Benutzer in todool hochgeladenen Daten und Dokumente werden über einen zertifizierten Archivierungsanbieter in einem digitalen Archiv gespeichert, in Übereinstimmung mit den geltenden Bestimmungen des Gesetzesdekrets Nr. 82 vom 7. März 2005 (Codice dell'Amministrazione digitale).

Artikel 5 – Ermächtigte Auftragsverarbeiter und Unter-Auftragsverarbeiter

5.1 – Der Auftragsverarbeiter identifiziert im Rahmen seiner Unternehmensstruktur die zur Datenverarbeitung berechtigten natürlichen Personen und gibt jeder zur Datenverarbeitung berechtigten Person Anweisungen über die Art der Behandlung, unter Einhaltung der Bestimmungen des GDPR Art. 28.

5.2 – Der Auftragsverarbeiter organisiert seine Tätigkeiten sowie die Schulung und Unterweisung seines Personals so, dass es der Ausführung des Vertrages dienlich ist und den Vorschriften der GDPR entspricht, sowie im Allgemeinen der Gesetzgebung zum Schutz personenbezogener Daten und Bestimmungen der Aufsichtsbehörde. Beispielsweise schreibt der Auftragsverarbeiter bei der schriftlichen Benennung der zur Datenverarbeitung berechtigten Personen vor, dass diese nur Zugang zu personenbezogenen Daten haben, deren Kenntnis zur Erfüllung der ihnen übertragenen Aufgaben unbedingt erforderlich ist. Der Auftragsverarbeiter überprüft auch, dass alle Verarbeiter alle Bestimmungen über die Sicherheit im Zusammenhang mit der Verwahrung der Schlüsselwörter (elektronische Verarbeitungen) anwenden und dass sie die nicht-elektronischen Datenträger, die Akten und Dokumente besonderer Kategorien personenbezogener Daten enthalten, an einem sicheren Ort aufbewahren, durch die Verwendung von verschließbaren Behältern (Papierbehandlung von Daten, die zu besonderen Kategorien gehören oder in jedem Fall ein höheres Risiko beinhalten).

5.3 – Der Auftragsverarbeiter verpflichtet die zur Durchführung der Verarbeitung befugten Personen auch für die Zeit nach Beendigung ihrer Beziehung zum Auftragsverarbeiter zur Vertraulichkeit in Bezug auf die von ihnen durchgeführten Vorgänge und in jedem Fall auf die personenbezogenen Daten, von denen sie Kenntnis erlangen oder die sie besitzen.

5.4 – Soweit erforderlich und soweit es sich um die Verarbeitung durch Personen handelt, die als „Systemadministrator“ zur Datenverarbeitung befugt sind, hat der Auftragsverarbeiter auch die geltenden Bestimmungen über die Regeln für Systemadministratoren einzuhalten, einschließlich derjenigen, die in der vom Datenschutzbeauftragten am 27. November 2008 erlassenen Bestimmung enthalten

sind, geändert auf der Grundlage der Bestimmung vom 25. Juni 2009, und in jedem Fall gemäß den Bestimmungen der Aufsichtsbehörde. Insbesondere verpflichtet sich der Auftragsverarbeiter, die Identifikationsdaten der verantwortlichen natürlichen Personen als Systemadministratoren direkt und gezielt aufzubewahren und auf Verlangen dem Inhaber der Datenverarbeitung unverzüglich zur Verfügung zu stellen.

5.5 – Der Auftragsverarbeiter kann sich im Falle einer vorherigen schriftlichen Genehmigung des Verantwortlichen gemäß den Bestimmungen des Art. 28 Absatz 2 der GDPR wiederum an zusätzliche Auftragsverarbeiter („**Unter-Auftragsverarbeiter**“) wenden. Mit diesem Schreiben erteilt der Verantwortliche dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung, damit dieser auf andere Auftragsverarbeiter zurückgreifen kann, wobei der Auftragsverarbeiter verpflichtet ist, den Verantwortlichen über geplante Änderungen bezüglich des Hinzufügens oder Ersetzens anderer Auftragsverarbeiter zu informieren, wodurch der Verantwortliche die Möglichkeit hat, solchen Änderungen zu widersprechen.

Derzeit greift der Auftragsverarbeiter auf folgende Unter-Auftragsverarbeiter zurück:

- Amazon AWS (für Hosting), <https://aws.amazon.com/it>
- Sarix GmbH (für Entwicklung und Wartung der Software), <https://www.sarix.eu>

5.6 – Für den Fall, dass der Auftragsverarbeiter auf Unter-Auftragsverarbeiter zurückgreift – auf der Grundlage der Bestimmungen des vorherigen Artikels 5.5 – muss der Verantwortliche selbst die Unter-Auftragsverarbeiter aus jenen Personen auswählen, die aufgrund ihrer Erfahrung, Fähigkeit und Zuverlässigkeit ausreichende Garantien bieten, um technische und organisatorische Maßnahmen so umzusetzen, dass die Verarbeitung den Anforderungen der geltenden Rechtsvorschriften entspricht und den Schutz der Rechte der betroffenen Personen gewährleistet.

Der Auftragsverarbeiter verpflichtet sich darüber hinaus, mit den Unter-Auftragsverarbeitern spezifische Verträge oder andere Rechtsakte mit dem Mindestinhalt gemäß Art. 28 Absatz 3 der GDPR abzuschließen, die die Aufgaben und Pflichten der Unter-Auftragsverarbeiter vorschreiben und diesen die Einhaltung der gleichen Pflichten auferlegen, unter Bezugnahme auf die Vorschriften über den Schutz personenbezogener Daten, die der Verantwortliche dem Auftragsverarbeiter gemäß den Rechtsvorschriften und den geltenden Maßnahmen der Aufsichtsbehörde auferlegt. Insbesondere müssen ausreichende Sicherheitsvorkehrungen getroffen werden, um geeignete technische und organisatorische Maßnahmen zu ergreifen, damit die Verarbeitung den Anforderungen dieses Gesetzes entspricht und in jedem Fall so, dass die Behandlung den Anforderungen der GDPR entspricht (Artikel 28 Absatz 4 GDPR). Der Auftragsverarbeiter trägt die volle Verantwortung gegenüber dem Verantwortlichen – unbeschadet einer direkten Handlung des Verantwortlichen

gegenüber den Unter-Auftragsverarbeitern, die gemeinsam mit dem Auftragsverarbeiter für die Gesamtschuld haften – für die Nichteinhaltung der Verpflichtungen der zusätzlichen Verantwortlichen hinsichtlich des Schutzes von Daten; falls erforderlich, verpflichtet sich der Auftragsverarbeiter daher ausdrücklich, den Verantwortlichen von jeglichen Forderungen, Entschädigungen, Sanktionen und/oder Schäden, die dem Verantwortlichen aus der Nichteinhaltung dieser Verpflichtungen entstehen könnten, und im Allgemeinen von der Verletzung des anwendbaren Gesetzes zum Schutz personenbezogener Daten durch den vom Auftragsverarbeiter ernannten Unter-Auftragsverarbeiter, auch mit der spezifischen Zustimmung des Verantwortlichen, zu entbinden.

Artikel 6 – Unterstützung des Verantwortlichen

6.1 – Der Auftragsverarbeiter verpflichtet sich, den für die Datenverarbeitung Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der GDPR genannten Rechte der betroffenen Person nachzukommen. Sollte der Auftragsverarbeiter auch über einen seiner Beauftragten Anträge auf Wahrnehmung der in Kapitel III der GDPR genannten Rechte der betroffenen Person entgegennehmen, hat er insbesondere für folgende Schritte zu sorgen:

- Umgehende Information des Verantwortlichen durch Beifügen einer Kopie des Antrages in Anlage;
- Einhaltung der entsprechenden praktischen Anweisungen, die er vom Verantwortlichen erhält;
- Sicherstellen, dass die Suche nach Informationen schnell und vollständig erfolgt.

6.2 – Der Auftragsverarbeiter verpflichtet sich, den für die Verarbeitung Verantwortlichen bei der Erfüllung der in Abschnitt 3 „Datenschutzfolgenabschätzung und vorherige Konsultation“ Artikel 32 bis 36 des GDPR genannten Verpflichtungen zu unterstützen, wobei er die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

6.3 – Der Auftragsverarbeiter kommt – nach rechtzeitiger Konsultation des Verantwortlichen – in der gesetzlich vorgeschriebenen Weise den Vorgaben der Datenschutzbehörde oder der ordentlichen Justiz nach und arbeitet mit dem Verantwortlichen bei der Umsetzung der ihm auferlegten Vorgaben zusammen.

6.4 – Der Auftragsverarbeiter leistet dem Verantwortlichen, sollte der Verantwortliche eine entsprechende Anfrage an ihn richten, auf dessen Kosten

Beistand bei seiner Verteidigung in Verfahren vor der Datenschutzbehörde oder vor der ordentlichen Justiz.

Artikel 7 – Meldung von Verletzungen

7.1 – Soweit es (tatsächlich eingetretene oder denkbare) Verletzungen des Schutzes von personenbezogenen Daten im Zusammenhang mit dem Dienst oder der vorliegenden Ernennung angeht, die den Auftragsverarbeiter (oder einen Unter-Auftragsverarbeiter) betreffen, hat der Auftragsverarbeiter die folgenden Pflichten:

- a) Umgehende Meldung der Verletzung gegenüber dem Verantwortlichen, sobald er Kenntnis hiervon erlangt hat, und
- b) Weiterleitung so bald als möglich (aber in jedem Fall spätestens innerhalb von 24 Stunden ab dem Zeitpunkt, zu dem man vom Vorliegen besagter Verletzung erfahren hat) an den Verantwortlichen aller Einzelheiten, die der Verantwortliche vernünftigerweise zu folgenden Punkten verlangen kann:
 - zur Art der Verletzung mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der archivierten personenbezogenen Daten;
 - zu jeglicher die besagte Verletzung betreffenden Ermittlung;
 - zu den wahrscheinlichen Folgen der Verletzung; und
 - zu jeglicher Maßnahme, die der Auftragsverarbeiter ergriffen oder vorgeschlagen hat, um die Verletzung zu beheben, einschließlich der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen und zur Vermeidung des neuerlichen Auftretens der gleichen oder ähnlicher Verletzungen.

Sollte der Auftragsverarbeiter berechtigterweise davon ausgehen, dass eine Weiterleitung der vorstehend genannten Spezifikationen innerhalb der vorgesehenen Frist nicht möglich ist, ist er zu folgenden Handlungen verpflichtet: Er hat dem Verantwortlichen – vor Ablauf der betreffenden Frist – die Gründe für die Verzögerung und die Frist zu nennen, innerhalb der er es für möglich hält, die entsprechenden Spezifikationen weiterleiten zu können (die Spezifikationen können auch zeitlich versetzt weitergeleitet werden), und er hat den Verantwortlichen, soweit es diesen Punkt betrifft, regelmäßig auf den neuesten Stand zu bringen; außerdem hat er dem Verantwortlichen jegliche Zusammenarbeit und Unterstützung zu gewährleisten, die im Zusammenhang mit Rechtsbehelfen notwendig sein sollte, wozu auch die Meldung gegenüber den natürlichen Personen, deren personenbezogene Daten von der Verletzung betroffen sind, zählt (nach Erteilung der Genehmigung durch den Verantwortlichen).

7.2 – Der Verantwortliche behält sich das Recht vor, die Verletzung innerhalb von 72 Stunden an die Aufsichtsbehörde zu übermitteln (vgl. Art. 33 GDPR); dies gilt auch für vom Auftragsverarbeiter stammende Mitteilungen.

Artikel 8 – Inspektionen und Untersuchungen

8.1 – Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen alle Informationen zur Verfügung zu stellen, die notwendig sind, um die Einhaltung der Pflichten laut Art. 28 der GDPR nachzuweisen, außerdem ermöglicht er die Überprüfungen einschließlich der vom Verantwortlichen durchgeführten Inspektionen und trägt zu diesen bei.

8.2 – Insbesondere kann der Verantwortliche jederzeit Untersuchungen und Inspektionen an den Orten durchführen, an denen die Datenverarbeitungsvorgänge stattfinden oder an denen die personenbezogenen Daten oder die Dokumentation im Zusammenhang mit vorliegendem Rechtsakt aufbewahrt werden. Diese Untersuchungen dürfen nur von qualifiziertem Personal des Verantwortlichen durchgeführt werden.

8.3 – Der Verantwortliche übermittelt dem Auftragsverarbeiter schriftlich das Datum und den Namen der Personen, welche die Inspektion und Prüfung in seinem Namen durchführen werden. Es wird vorausgesetzt, dass eine solche Inspektion so durchgeführt wird, dass der normale Geschäftsablauf des Auftragsverarbeiters nicht beeinträchtigt wird, und dass der Auftragsverarbeiter in angemessener Weise davon in Kenntnis gesetzt wird.

Artikel 9 – Entgelt und Haftung

9.1 – Das vorliegende Schreiben oder die Rolle der Auftragsverarbeiter impliziert keinen Anspruch auf eine weitere Vergütung als in dem Vertrag vorgesehen, oder auf den Preis von Dienstleistungen oder Lieferungen in Bezug auf die Anweisungen des Verantwortlichen (zu diesem letzten Aspekt wird von Zeit zu Zeit ein spezifisches Angebot formuliert).

9.2 – Eine Partei, die gegen ihre Verpflichtungen aus diesem Schreiben oder andere datenschutzrechtliche Verpflichtungen verstößt, hat die andere Partei von allen Schäden, Ansprüchen, Entschädigungen, Strafen und/oder anderen Schäden schadlos zu halten, die der anderen Partei aus einem solchen Verstoß entstehen können.

Artikel 10 – Mitteilungen

10.1 – Die im Zusammenhang mit der vorliegenden Beauftragung vorzunehmenden Mitteilungen sind folgendermaßen zu adressieren:

Mitteilungen an den Verantwortlichen:

Bei der Anmeldung zum Dienst angegebene Daten des Verantwortlichen.

Mitteilungen an den Auftragsverarbeiter:

todool GmbH

Sterngasse 6

39052 Kaltern an der Weinstraße (BZ)

PEC: todool@pec.it

10.2 – Etwaige Änderungen an den im voranstehenden Absatz aufgeführten Daten müssen umgehend gemeldet werden.

Artikel 11 – Beginn und Dauer der Beauftragung

11.1 – Der Inhalt des vorliegenden Schreibens ist ab dem heutigen Datum gültig.

11.2 – Bei Beendigung des zwischen den Parteien bestehenden Vertrages, aus jedwedem Grund, endet auch die Legitimation der Auftragsverarbeiter, unbeschadet der Zeit, die erforderlich ist, um die Vorgänge einer eventuellen Migration der Daten zum Verantwortlichen abzuschließen, und in jedem Fall der Löschung der Dokumentation und der Daten durch den Auftragsverarbeiter, wie im Vertrag geregelt (siehe insbesondere Art. 11.5 der Allgemeinen Geschäftsbedingungen).