

ATTO DI REGOLAMENTAZIONE DELLA DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679 (GDPR)

tra

il **Cliente**, come identificato nelle Condizioni Generali del Contratto di servizio todool, di seguito anche **"Titolare del trattamento"** o solo **"Titolare"**

e

todool s.r.l., con sede legale in 39052 Caldaro sulla strada del vino (BZ), Vicolo Stella 6, Partita IVA 03085210213, PEC: todool@pec.it, di seguito anche **"Responsabile del trattamento"** o solo **"Responsabile"**.

Premesse e definizioni

- a) Il Titolare del trattamento e il Responsabile del trattamento (entrambe collettivamente definite anche **"Parti"**) hanno stipulato il Contratto di servizio per l'applicazione todool la cui esecuzione comporta il trattamento di dati personali da parte del Responsabile per conto del Titolare;
- b) il Responsabile possiede adeguati requisiti di esperienza, capacità e affidabilità sufficienti per mettere in atto misure tecniche e organizzative adeguate e per svolgere il ruolo di responsabile esterno del trattamento dei dati personali;
- c) con la presente scrittura, le Parti intendono regolamentare i rispettivi obblighi nell'ambito del trattamento di cui alla precedente lettera a) (**"Trattamento"**), in particolare vincolando il Responsabile del trattamento al Titolare del trattamento e stipulando la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
- d) se nella presente scrittura sono utilizzati termini a cui il Regolamento (UE) 2016/679 (**"GDPR"**) attribuisce una definizione, a tali termini andrà dato tale specifico significato, fermo che quanto indicato nella presente scrittura non modifica o interferisce con le definizioni di cui al Contratto, che rimangono quindi inalterate; ai sensi del presente atto, il soggetto designante viene definito Titolare, indipendentemente dal fatto che per determinati dati personali possa in concreto ricoprire esso stesso il ruolo di Responsabile del trattamento rispetto da altro Titolare del trattamento; se non diversamente indicato, inoltre, per **"Dati personali"** e **"Interessati"** devono intendersi rispettivamente i dati personali trattati dal Responsabile per conto del Titolare e i soggetti a cui si riferiscono tali

dati. Per **“Dati trasmessi”** (e quindi i collegati termini quali trasmissione dei dati ecc.) devono intendersi dati personali trattati dal Responsabile per conto del Titolare da quest’ultimo direttamente comunicati o che terzi o gli Interessati hanno trasmesso al Responsabile su indicazione del Titolare;

e) la presente scrittura integra il Contratto in relazione allo scopo di cui al precedente punto c) delle premesse, rimanendo per il resto inalterato il contenuto del Contratto medesimo.

Articolo 1 – Definizione del ruolo

1.1 – todool s.r.l. assume la qualifica di Responsabile del trattamento, e ad essa sono affidate tutte – ed esclusivamente – le operazioni di trattamento dei dati personali necessarie per dare esecuzione all’incarico di cui al Contratto. Le finalità del trattamento sono connesse alla gestione degli adempimenti fiscali dei soggetti (che sono quindi gli Interessati) rispettivamente ai quali il Titolare utilizza l’applicazione todool. I dati oggetto di trattamento possono appartenere sia alla categoria dei dati comuni che a particolari categorie di dati (in particolare dati relativi alla salute).

1.2 – Le operazioni di trattamento sono effettuate utilizzando supporti di tipo informatico.

1.3 – Il Responsabile del trattamento è tenuto a trattare i dati personali nel rispetto dei principi e delle disposizioni del GDPR, della normativa sulla protezione dei dati personali in genere e dei provvedimenti della competente Autorità di Controllo, e, comunque, solo su istruzione documentata del Titolare.

1.4 – Il Responsabile provvede inoltre a dare esecuzione agli obblighi che il GDPR e comunque la normativa, nonché i provvedimenti della competente Autorità di Controllo, pongono direttamente a suo carico.

Articolo 2 – Dichiarazioni e garanzie del Titolare

2.1 – Il Titolare dichiara che i dati personali che ha trasmesso e che trasmetterà al Responsabile sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati, nonché che essi sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile. Si precisa che rimane a carico del Titolare l’onere di individuare la base giuridica del trattamento dei dati personali.

Articolo 3 – Obblighi, dichiarazioni e garanzie del Responsabile

3.1 – Fermo quanto sopra e le disposizioni di cui ai successivi articoli, il Responsabile si impegna, dichiara e garantisce che:

- i dati personali oggetto di trattamento saranno costituiti esclusivamente dai dati comunicati dal Titolare e il Responsabile non potrà utilizzare nessuna diversa forma di acquisizione dei dati personali predetti;
- per gli obblighi di propria pertinenza, effettuerà il trattamento dei dati personali nel rispetto delle finalità e modalità decisi dal Titolare.

Articolo 4 – Misure di sicurezza

4.1 – Il Responsabile adotta le misure di sicurezza e salvaguardia della riservatezza dei dati personali, adeguate a ridurre al minimo i rischi di distruzione o perdita intenzionale o accidentale dei dati, di accesso non autorizzato, di trattamento non consentito e di trattamento non conforme alle finalità dichiarate.

4.2 – Il Responsabile si impegna in ogni caso all'adeguamento dei propri sistemi alle misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, come previsto dal GDPR all'art. 32, e a verificarne periodicamente il rispetto. In ogni caso, dovranno essere rispettate le seguenti misure di sicurezza:

- quanto alla riservatezza dei dati personali:
 - a) protezione fisica dei locali e degli apparati con cui avviene il trattamento
 - b) sicurezza degli accessi fisici e logici
 - c) assegnazioni di adeguati privilegi di accesso ai dati
 - d) utilizzo di tecniche di crittografia
 - e) eliminazione sicura dei documenti fisici e digitali
- quanto all'integrità dei dati personali:
 - a) protezione nella trasmissione dei dati
 - b) sicurezza dell'elaborazione dei dati
 - c) protezione dei sistemi informatici
- quanto alla disponibilità dei dati personali:
 - a) politiche di backup
 - b) piani di business continuity.

I dati e documenti caricati dall'utente in todool vengono memorizzati in un archivio digitale tramite un provider certificato di archiviazione, in conformità alle disposizioni applicabili del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale).

Articolo 5 – Soggetti autorizzati e Sub-Responsabili del trattamento

5.1 – Il Responsabile, nell'ambito della propria struttura aziendale, individua le persone fisiche autorizzate al trattamento e, contestualmente, fornisce a ciascun autorizzato

alle operazioni di trattamento istruzioni circa le modalità del trattamento medesimo, in ottemperanza a quanto disposto dall'art. 28 del GDPR.

5.2 – Il Responsabile organizza le proprie attività e predispone la formazione e l'istruzione del proprio personale in modo compatibile e funzionale all'esecuzione del Contratto e alle prescrizioni del GDPR, in generale della normativa relativa alla protezione dei dati personali e ai provvedimenti dell'Autorità di Controllo. A titolo esemplificativo e non esaustivo, il Responsabile, nel designare per iscritto le persone autorizzate al trattamento, prescrive che esse abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati; verifica, inoltre, che le stesse applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave (trattamenti elettronici) e che conservino in luogo sicuro i supporti non informatici contenenti atti o documenti con categorie particolari di dati o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei di dati appartenenti a particolari categorie o comunque comportanti maggiore rischio).

5.3 – Il Responsabile vincola, anche per il tempo successivo alla cessazione del loro rapporto con il Responsabile medesimo, i soggetti autorizzati alle attività di trattamento alla riservatezza in relazione alle operazioni dagli stessi eseguite, e in ogni caso ai dati personali di cui essi dovessero comunque venire a conoscenza o in possesso.

5.4 – Ove occorrer possa e per quanto concerna i trattamenti effettuati dalle persone autorizzate al trattamento con mansioni di "Amministratore di Sistema", il Responsabile è tenuto pure al rispetto delle previsioni applicabili relative alla disciplina sugli amministratori di sistema, anche come contenute nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009 e comunque secondo il provvedimento dell'Autorità di Controllo. Il Responsabile, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.

5.5 – Il Responsabile potrà ricorrere a propria volta a ulteriori responsabili del trattamento ("**Sub-Responsabili**"). Con la presente scrittura, il Titolare conferisce autorizzazione scritta generale al Responsabile a poter ricorrere a eventuali ulteriori responsabili del trattamento ("**Sub-Responsabili**"), con obbligo del Responsabile di informare il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Il Responsabile attualmente ricorre ai seguenti Sub-Responsabili:

- Amazon AWS (per hosting), <https://aws.amazon.com/it>
- Sarix s.r.l. (per sviluppo e manutenzione software), <https://www.sarix.eu>

5.6 – Nel caso in cui il Responsabile faccia ricorso a Sub-Responsabili – quindi sulla base di quanto previsto al precedente articolo 5.5 – il Responsabile medesimo dovrà selezionare i Sub-Responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di cui alla normativa applicabile e garantisca la tutela dei diritti degli Interessati. Il Responsabile si impegna altresì a stipulare con i Sub-Responsabili specifici contratti, o altri atti giuridici, aventi il contenuto minimo di cui all’art. 28 paragrafo 3 GDPR, che prescrivano analiticamente i compiti e obblighi di questi ultimi e impongano a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali, imposti dal Titolare al Responsabile ai sensi della normativa e degli applicabili provvedimenti della competente Autorità di Controllo, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente atto e in ogni caso in modo tale che il trattamento soddisfi i requisiti del GDPR (art. 28 paragrafo 4, GDPR). Il Responsabile mantiene verso il Titolare l’intera responsabilità – ferma comunque un’azione diretta del Titolare verso i Sub-Responsabili, che saranno responsabili in solido con il Responsabile verso il Titolare – per inadempimenti dei Sub-Responsabili agli obblighi in materia di protezione dei dati; per quanto occorrer possa, quindi, il Responsabile si impegna espressamente a risarcire, manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, sanzione e/o comunque pregiudizio che possa derivare al Titolare medesimo dalla mancata osservanza di tali obblighi e, in generale, dalla violazione della applicabile normativa sulla tutela dei dati personali da parte dei Sub-Responsabili nominati dal Responsabile, quand’anche con il consenso, anche specifico, del Titolare.

Articolo 6 – Assistenza al Titolare

6.1 – Il Responsabile si impegna ad assistere il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l’obbligo del Titolare del trattamento di dare seguito alle richieste per l’esercizio da parte degli Interessati dei diritti di cui al capo III del GDPR. In particolare, nel caso in cui il Responsabile riceva, anche per il tramite di un suo Incaricato, richieste riconducibili all’esercizio dei diritti dell’Interessato di cui al capo III del GDPR, provvede a:

- informare senza ritardo il Titolare, allegando copia della richiesta;

- attenersi alle istruzioni operative che riceve in merito dal Titolare;
- fare in modo di assicurare che le operazioni di ricerca delle informazioni, di cui è in possesso, siano rapide e complete.

6.2 – Il Responsabile si impegna ad assistere il Titolare nel garantire il rispetto degli obblighi di cui alla sezione 3 “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva” agli artt. da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a propria disposizione.

6.3 – Il Responsabile – previa tempestiva consultazione con il Titolare – adempie, a norma di legge, alle prescrizioni provenienti dall’Ufficio del Garante o dall’Autorità Giudiziaria Ordinaria e collabora con il Titolare per l’attuazione delle prescrizioni a questi impartite.

6.4 – Il Responsabile, su richiesta eventuale del Titolare e a spese dello stesso, coadiuva quest’ultimo nella difesa nei procedimenti dinanzi al Garante o all’Autorità Giudiziaria Ordinaria.

Articolo 7 - Segnalazione delle violazioni

7.1 – Per quanto concerne qualsivoglia violazione (effettiva o potenziale) di dati personali relativa al Servizio o alla presente Nomina che coinvolga il Responsabile (o un Sub-Responsabile del trattamento), il Responsabile dovrà:

- a) segnalare al Titolare senza indugio la violazione dal momento in cui abbia conoscenza della medesima; e
- b) fornire al Titolare non appena possibile (ma in ogni caso al più tardi entro 24 ore dal momento in cui si sia appreso dell’esistenza della suddetta violazione) tutte le specifiche che il Titolare possa ragionevolmente richiedere in merito:
 - alla natura della violazione, comprese le tipologie e il numero approssimativo di Interessati e dati personali archiviati coinvolti;
 - a qualsivoglia indagine riguardante la suddetta violazione;
 - alle probabili conseguenze derivanti dalla violazione; e
 - a qualsivoglia misura adottata o raccomandata dal Responsabile per porre rimedio alla violazione, comprese quelle volte a contenere le eventuali conseguenze negative derivanti da tale violazione e quelle volte a prevenire il ripresentarsi della stessa violazione o di violazioni simili.

Tuttavia, qualora il Responsabile ritenga ragionevolmente che non sia possibile fornire le suddette specifiche nel termine previsto, lo stesso sarà tenuto – prima della scadenza del termine in questione – a indicare al Titolare i motivi del ritardo e il termine entro cui ritenga di poter fornire le relative specifiche (che potranno anche

essere fornite scaglionate nel tempo) e a tenere periodicamente aggiornato il Titolare sul punto; nonché fornire al Titolare la collaborazione e l'assistenza necessarie in merito a qualsivoglia rimedio giurisdizionale da adottare, compresa qualsivoglia segnalazione alle persone fisiche i cui dati personali siano coinvolti nella violazione (previa autorizzazione da parte del Titolare).

7.2 – Il Titolare si riserva il diritto di notificare la violazione all'Autorità di Controllo entro 72 ore (ex Art. 33 GDPR), e qualsivoglia comunicazione proveniente dal Responsabile.

Articolo 8 – Ispezioni e controlli

8.1 – Il Responsabile si impegna a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR e consente e contribuisce alle attività di revisione, comprese le ispezioni effettuate dal Titolare.

8.2 – In particolare il Titolare ha facoltà di effettuare in ogni momento controlli e ispezioni nei luoghi dove hanno svolgimento le operazioni di trattamento o dove sono custoditi i dati personali o la documentazione relativi al presente atto. I suddetti controlli potranno essere effettuati esclusivamente da personale qualificato del Titolare.

8.3 – Il Titolare notifica per iscritto al Responsabile la data e il nominativo delle persone che, per suo conto, effettueranno le operazioni di ispezione e revisione. Resta inteso che qualsiasi verifica dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un ragionevole preavviso.

Articolo 9 – Corrispettivo e responsabilità

9.1 – La presente scrittura o comunque il ruolo di responsabile del trattamento dei dati personali non comporta alcun diritto del Responsabile a compenso ulteriore rispetto a quanto previsto dal Contratto, o al prezzo degli eventuali servizi o forniture eventualmente necessari in relazione alle istruzioni del Titolare (in merito a tale ultimo aspetto, verrà di volta in volta formulata specifica offerta con preventivo).

9.2 – La Parte che violi i propri obblighi di cui alla presente scrittura o comunque gli obblighi connessi alla normativa sulla tutela dei dati personali, sarà tenuta a risarcire, manlevare e tenere indenne l'altra Parte da qualsiasi danno, pretesa, risarcimento, sanzione e/o comunque pregiudizio che possa derivare a quest'ultima da tale violazione.

Articolo 10 – Comunicazioni

10.1 – Ogni comunicazione da effettuare ai fini del presente incarico dovrà essere inviata a:

per il Titolare:

Dati del Titolare indicati al momento della sottoscrizione del Servizio.

per il Responsabile:

todool s.r.l.
Vicolo Stella, 6
39052 Caldaro sulla strada del vino (BZ)
PEC: todool@pec.it

10.2 – Eventuali modifiche dei dati di cui al precedente comma dovranno essere tempestivamente segnalate.

Articolo 11 – Decorrenza e durata

11.1 – Quanto oggetto della presente scrittura ha decorrenza dalla data odierna.

11.2 – Alla cessazione del Contratto in essere tra le Parti, per qualsiasi causa intervenuta, cesserà immediatamente la legittimazione del Responsabile al trattamento, fatto salvo il tempo necessario a completare le operazioni di eventuale migrazione dei dati al Titolare e comunque di cancellazione della documentazione e dei dati da parte del Responsabile come regolamentato dal Contratto (cfr. in particolare art. 11.5 delle Condizioni Generali di Contratto).