# **DPA - ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI**

TRA:

Il Cliente, in qualità di Titolare/Contitolare/Responsabile del trattamento dei dati personali;

Onirys S.r.l., con sede legale in via Larga 27/4C Bologna, P.IVA 04298431208, in qualità di Fornitore, Responsabile Esterno del trattamento ai sensi dell’art. 28 GDPR.

# **Art. 1 – OGGETTO E SCOPO DEL DOCUMENTO**

1.1 Il presente DPA ha ad oggetto le modalità e le condizioni di trattamento dei dati personali (di seguito, “Dati”) di cui il Cliente è Titolare / Contitolare ovvero che tratta in qualità di Responsabile del trattamento, rispetto ai quali nomina **Onirys S.r.l.** (di seguito anche solo “Fornitore”), quale Responsabile esterno del trattamento, limitatamente alle operazioni effettuate nell’ambito dei servizi erogati in esecuzione del Contratto stipulato tra le Parti, di cui il presente DPA costituisce parte integrante.

1.2 In particolare, con il presente atto il Cliente designa formalmente il Fornitore quale Responsabile esterno del trattamento, in relazione alle attività di trattamento effettuate nell’ambito dell’utilizzo del servizio e della piattaforma di automazione vocale intelligente realizzata da Onirys.

1.3 Il Fornitore opererà dunque in qualità di Responsabile esterno del trattamento, ai sensi dell’art. 4, comma 1, punto 8 del GDPR, mentre il Cliente continuerà ad agire nella propria qualità di Titolare / Contitolare / Responsabile del trattamento ai sensi dell’art. 4, comma 1, punto 7 del GDPR, secondo i casi.

1.4 Ciascuna parte si impegna a rispettare i doveri e gli obblighi previsti dal GDPR e dalla normativa nazionale applicabile in materia di protezione dei dati personali, nell’ambito del trattamento di cui al presente DPA.

1.5 Con la sottoscrizione del presente atto, il Cliente autorizza il Fornitore a trattare i Dati esclusivamente in conformità a quanto stabilito dalla normativa applicabile, e specificamente:
 (a) per l’erogazione dei servizi richiesti dal Cliente;
 (b) secondo quanto previsto nel Contratto e nella documentazione contrattuale ad esso collegata;
 (c) secondo le ulteriori istruzioni scritte eventualmente fornite dal Cliente e formalmente accettate dal Fornitore, purché compatibili con la normativa vigente.

1.6 Il Fornitore si impegna a rispettare le istruzioni di trattamento contenute nel presente documento. Il Cliente garantisce di aver raccolto i Dati in modo lecito, trasparente e nel rispetto della normativa, e in particolare di aver fornito agli interessati tutte le informazioni richieste dagli articoli 13 e 14 del GDPR.

1.7 Qualora il Cliente intenda utilizzare i Servizi in modo difforme da quanto descritto nel presente documento, e ciò comporti un diverso inquadramento giuridico del trattamento, è tenuto a darne preventiva comunicazione scritta al Fornitore. Quest’ultimo valuterà la situazione al fine di apportare eventuali modifiche contrattuali o tecniche, anche con riferimento alla sicurezza del trattamento.

1.8 Qualora il Cliente agisca in qualità di Responsabile del trattamento, egli garantisce che tutte le istruzioni impartite al Fornitore, inclusa la nomina di quest’ultimo in qualità di ulteriore Responsabile, siano state previamente autorizzate dal Titolare del trattamento.

1.9 Il presente DPA non comporta alcun obbligo per il Fornitore di prestare servizi ulteriori rispetto a quanto previsto dal Contratto. Qualora il Cliente ravvisi la necessità di ulteriori misure per garantire la conformità normativa, comprese misure tecniche o organizzative supplementari, dovrà farne richiesta formale al Fornitore, il quale fornirà un’offerta economica separata per tali attività, che non saranno considerate automaticamente incluse nei servizi contrattuali.

# **Art. 2 – SICUREZZA**

2.1 Il Fornitore si impegna ad adottare tutte le misure di sicurezza previste dalla normativa vigente in materia di protezione dei Dati personali, nonché dai provvedimenti emessi dall’Autorità Garante, al fine di assicurare la protezione dei Dati da trattamenti non autorizzati o illeciti, nonché da perdita, distruzione, divulgazione o accesso accidentali o intenzionali.

2.2 Il Fornitore applica misure di sicurezza tecniche, organizzative e logiche che sono descritte nel Contratto, negli allegati tecnici, nell’Allegato “A” del presente DPA e nella documentazione operativa resa disponibile al Cliente.

2.3 Tali misure comprendono, tra l’altro:

· garanzie sulla riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi;

· capacità di ripristino tempestivo dei Dati in caso di incidente;

· processi di test, verifica e valutazione regolari per assicurare l’efficacia delle misure implementate.
 Il Fornitore potrà aggiornare tali misure nel tempo, purché i cambiamenti non ne riducano l’efficacia complessiva.

2.4 Il Fornitore assicura che il proprio personale, nonché eventuali appaltatori e Sub-responsabili, sia tenuto a rispettare le misure di sicurezza in funzione dei rispettivi ambiti di competenza.

2.5 Il Cliente riconosce che le misure tecniche e organizzative adottate e mantenute dal Fornitore risultano adeguate a garantire un livello di sicurezza proporzionato ai rischi connessi al trattamento dei Dati personali.

2.6 In caso di aggiornamento delle misure di sicurezza, il Fornitore ne darà comunicazione al Cliente con i mezzi ritenuti più idonei. Il Cliente potrà, in tali casi, richiedere un elenco aggiornato delle misure applicate.

2.7 Il Cliente resta unico responsabile per l’utilizzo dei Servizi, e in particolare per:

· adottare misure idonee a garantire un livello di sicurezza adeguato in relazione ai Dati trattati;

· proteggere credenziali, sistemi e dispositivi di autenticazione utilizzati per accedere ai Servizi;

· eseguire backup periodici dei Dati anche mediante strumenti propri e/o off-line.

2.8 Il Fornitore non è tenuto a proteggere i Dati eventualmente archiviati o trasferiti dal Cliente al di fuori dei propri sistemi (es. archiviazione locale o cloud terzi), né ad applicare misure ulteriori rispetto a quelle contrattualmente previste.[LD1]

2.9 È responsabilità esclusiva del Cliente valutare se i Servizi e le misure di sicurezza adottate dal Fornitore soddisfino i requisiti previsti dal GDPR, tenuto conto della natura, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà degli interessati. Qualora il Cliente ritenga necessarie misure aggiuntive, sarà tenuto a richiederle e sostenerne i costi. In difetto, manleverà il Fornitore da ogni responsabilità derivante dalla mancata adozione delle suddette misure.

# **Art. 3 – TRASFERIMENTO DI DATI**

3.1 I Dati trattati dal Fornitore per l’erogazione dei Servizi di cui al presente DPA sono segregati a livello infrastrutturale e logico, all’interno di ambienti separati dedicati al Cliente. L’infrastruttura tecnologica utilizzata da Onirys è ubicata all’interno del territorio dell’Unione Europea, presso data center certificati che garantiscono standard di affidabilità e sicurezza idonei alla natura dei trattamenti svolti.

3.2 In linea generale, i Dati personali oggetto di trattamento non vengono trasferiti in Paesi situati al di fuori dello Spazio Economico Europeo (“SEE”). Qualora, per motivi tecnici o funzionali, si rendesse necessario effettuare un trasferimento verso Paesi terzi, il Fornitore si impegna a:

· privilegiare Paesi per i quali la Commissione Europea abbia emesso una decisione di adeguatezza ai sensi dell’art. 45 del GDPR;

· in alternativa, adottare le Clausole Contrattuali Standard approvate dalla Commissione Europea ai sensi dell’art. 46, par. 2, lett. c) del GDPR;

· adottare, ove necessario, misure supplementari tecniche, contrattuali o organizzative per garantire un livello di protezione sostanzialmente equivalente a quello previsto nel SEE.

3.3 Ogni trasferimento di Dati extra-SEE sarà oggetto di valutazione preventiva del rischio da parte del Fornitore, che informerà tempestivamente il Cliente qualora emergano criticità che possano compromettere l’adeguatezza del trattamento.

# **Art. 4 – ATTIVAZIONE ED EROGAZIONE DEI SERVIZI**

4.1 Con la sottoscrizione del presente DPA, il Cliente autorizza il Fornitore ad avvalersi di Sub-responsabili esterni per lo svolgimento di specifiche attività tecniche, infrastrutturali o operative, laddove necessario per garantire l’erogazione dei Servizi. Il Cliente riconosce e accetta che ciò possa comportare il trattamento dei Dati da parte di tali soggetti, sotto il controllo del Fornitore.

4.2 In tal caso, il Fornitore si impegna a stipulare con ciascun Sub-responsabile un contratto che:

· limiti il trattamento dei Dati alla sola esecuzione delle attività delegate dal Fornitore, nel rispetto del presente DPA e delle istruzioni del Cliente;

· imponga al Sub-responsabile il rispetto degli obblighi previsti dall’art. 28 del GDPR;

· confermi che il Fornitore rimanga pienamente responsabile nei confronti del Cliente per ogni attività svolta dal Sub-responsabile nell’ambito dei trattamenti delegati.

4.3 Al fine di garantire al Cliente pieno controllo sui soggetti coinvolti nelle attività di trattamento, il Fornitore mantiene un elenco aggiornato dei Sub-responsabili, che sarà reso disponibile al Cliente su sua richiesta scritta, unitamente alla documentazione che attesti il rispetto degli obblighi contrattuali e di legge da parte dei medesimi.

4.4 Il Fornitore si impegna inoltre a comunicare al Cliente, con congruo preavviso, ogni modifica sostanziale relativa all’elenco dei Sub-responsabili, affinché il Cliente possa esprimere eventuali osservazioni o obiezioni, che saranno oggetto di valutazione congiunta tra le Parti.

# **Art. 5 – VERIFICHE**

5.1 Il Fornitore si impegna a mettere a disposizione del Cliente tutte le informazioni necessarie a dimostrare la conformità del trattamento [LD2] alle disposizioni del GDPR e agli obblighi previsti dal presente DPA, nella misura in cui tali informazioni non implichino la divulgazione di Dati di soggetti terzi o violazioni di obblighi di riservatezza, anche in riferimento a segreti industriali o commerciali tutelati.

5.2 Il Cliente, o un soggetto da esso formalmente incaricato, ha il diritto di effettuare verifiche, ispezioni o audit volti ad accertare la conformità dell’operato del Fornitore rispetto agli obblighi assunti con il presente DPA e alla normativa applicabile in materia di protezione dei Dati. Tali verifiche dovranno essere concordate preventivamente con il Fornitore quanto a tempi, modalità e ambito di intervento, e non dovranno interferire con l’operatività ordinaria dei sistemi.

5.3 I costi relativi alle attività di verifica, incluse eventuali spese vive sostenute dal Fornitore per consentire l’accesso ai propri ambienti o per la preparazione della documentazione richiesta, saranno integralmente a carico del Cliente, salvo diversa pattuizione espressa.

5.4 Il Fornitore si impegna altresì a collaborare con il Cliente fornendo ogni informazione ragionevole utile a consentire la verifica della conformità delle misure di sicurezza applicate, come descritte nel Contratto e nell’Allegato “A”.

5.5 Il Cliente è tenuto a valutare autonomamente la necessità di effettuare una valutazione d’impatto sulla protezione dei dati (DPIA) ai sensi dell’art. 35 del GDPR, in relazione al tipo di trattamento effettuato tramite i Servizi. In tale eventualità, il Fornitore garantirà il supporto necessario, limitatamente al proprio ambito di responsabilità, per consentire al Cliente di adempiere agli obblighi previsti.

# **Art. 6 – RICHIESTE DEGLI INTERESSATI**

6.1 Qualora, durante la vigenza del Contratto, il Fornitore riceva richieste da parte di soggetti interessati (ai sensi degli articoli 15–22 del GDPR) relative ai Dati trattati per conto del Cliente, e risulti evidente che tali richieste riguardino esclusivamente trattamenti per i quali il Cliente è Titolare, il Fornitore informerà senza indugio l’interessato della necessità di rivolgere la propria richiesta direttamente al Cliente.

6.2 Ove il Cliente, per motivi tecnici, normativi o organizzativi, non sia in grado di evadere autonomamente una richiesta pervenuta da un interessato, il Fornitore si impegna a fornire il supporto necessario, nei limiti delle proprie competenze e capacità tecniche, affinché il Cliente possa soddisfare le richieste ricevute nel rispetto dei termini di legge.

6.3 Il Fornitore mette a disposizione del Cliente, compatibilmente con le funzionalità tecniche della propria piattaforma e nel rispetto delle condizioni contrattuali, strumenti adeguati per consentire:

· la rettifica o l’aggiornamento dei Dati;

· la cancellazione o limitazione del trattamento;

· il recupero dei Dati per esigenze di portabilità, secondo quanto previsto dalla normativa applicabile.

6.4 Resta inteso che tutte le attività di supporto fornite dal Fornitore in relazione alla gestione delle richieste degli interessati potranno essere oggetto di valorizzazione economica, qualora comportino uno sforzo significativo non previsto nel Contratto originario.

# **Art. 7 – VIOLAZIONE DI DATI PERSONALI**

7.1 Qualora, nell’ambito dell’erogazione dei Servizi, si verifichi un evento che comporti la violazione dei Dati personali trattati dal Fornitore per conto del Cliente (“Data Breach”), il Fornitore si impegna a informare tempestivamente il Cliente in conformità con quanto previsto dall’art. 33 del GDPR e dalla normativa applicabile.

7.2 In particolare, il Fornitore si impegna a fornire una comunicazione formale al Cliente entro 24 ore dalla conoscenza dell’evento, che dovrà contenere, ove possibile:

· una descrizione della natura della violazione, comprese le categorie e il numero approssimativo di interessati coinvolti, nonché il numero approssimativo di registrazioni di Dati personali oggetto della violazione;

· la descrizione delle probabili conseguenze della violazione;

· le misure adottate o proposte dal Fornitore per porre rimedio alla violazione e mitigarne i possibili effetti negativi;

· i dati di contatto di un referente interno del Fornitore incaricato della gestione dell’evento.

7.3 Il Cliente, in qualità di Titolare del trattamento, sarà responsabile di effettuare le notifiche eventualmente necessarie alle autorità competenti e/o agli interessati, salvo che le Parti abbiano concordato diversamente.

7.4 È fatto obbligo per entrambe le Parti di mantenere riservate tutte le informazioni relative alla violazione, incluse le comunicazioni intercorse in merito. Tali informazioni non potranno essere divulgate a terzi, se non nei casi imposti dalla legge o da esplicita richiesta di autorità pubbliche competenti.

# **Art. 8 – DURATA**

8.1 Il presente DPA avrà durata pari a quella del Contratto sottoscritto tra il Cliente e il Fornitore per l’erogazione dei Servizi, e cesserà automaticamente di avere efficacia in caso di risoluzione, recesso o scadenza del Contratto stesso, salvo quanto previsto al paragrafo seguente.

8.2 Alla cessazione del Contratto, il Fornitore garantirà al Cliente, per un periodo di tempo ragionevole concordato tra le Parti, l’accesso ai Dati personali trattati, al fine di consentirne il recupero o il trasferimento, secondo le modalità tecniche definite nel Contratto. Decorso tale termine, il Fornitore provvederà alla cancellazione o anonimizzazione dei Dati, salvo obblighi di conservazione previsti dalla legge.

8.3 In caso di rinnovo, esplicito o tacito, del Contratto principale, il presente DPA si considererà automaticamente prorogato per tutta la durata del rinnovo, salvo che una delle Parti non richieda per iscritto l’aggiornamento del contenuto del presente atto.

 [LD1]Spiegare come. Soluzione chiedi mandando una mail i dati

 [LD2]Come?