MASTER DATA PROCESSING AGREEMENT EX ART. 28 REGOLAMENTO UE 2016/679

ACCORDO PRINCIPALE PER IL TRATTAMENTO DEI DATI PERSONALI

1. RUOLI DELLE PARTI E AMBITO DI APPLICAZIONE

Il presente Master Data Processing Agreement (di seguito "MDPA") disciplina le condizioni e le modalità del trattamento dei dati personali eseguito da DEGG S.r.l. (di seguito il "Fornitore" o "Responsabile") nell'ambito dell'erogazione dei servizi (SaaS o Servizi Professionali) in favore del Cliente (di seguito il "Titolare"). Le Parti riconoscono e convengono che, ai sensi della normativa vigente, il **Fornitore** agisce quale **Responsabile del Trattamento** e il **Cliente** agisce quale **Titolare del Trattamento** in relazione ai dati personali immessi, conservati o elaborati tramite i servizi.

Le caratteristiche specifiche del trattamento (ivi incluse le categorie di dati, gli interessati, i tempi di conservazione e la lista specifica dei Sub-Responsabili) sono demandate e puntualmente descritte in separati documenti denominati "DPA - Condizioni Speciali". Tali documenti, declinati in base alla tipologia di servizio acquistato dal Titolare, costituiscono parte integrante ed essenziale del presente MDPA. Ai fini dell'assolvimento degli obblighi di forma scritta ex Art. 28, par. 9, GDPR e di conoscibilità ex Art. 1341 c.c., il Titolare dichiara di aver visionato, compreso e di accettare integralmente i "DPA - Condizioni Speciali" relativi ai servizi acquistati, resi costantemente disponibili da DEGG ai seguenti indirizzi web:

- DPA - Condizioni Speciali Servizi: www.degg.it/legal/dpa-servizi-professionali-v0100-09112026
- DPA - Condizioni Speciali DYNOS: www.degg.it/legal/dpa-dynosv0100-09112026
- DPA - Condizioni Speciali DWAY: www.degg.it/legal/dpa-dway-v0100-09112026
- DPA - Condizioni Speciali DBRAINS: www.degg.it/legal/dpa-dbrains-v0100-09112026
- DPA - Condizioni Speciali Factorial: www.degg.it/legal/dpa-factorial-v0100-09112026

2. OGGETTO E ISTRUZIONI DOCUMENTATE

Il Responsabile si impegna a trattare i dati personali esclusivamente sulla base delle istruzioni documentate del Titolare. Le Parti concordano espressamente che tali istruzioni documentate sono costituite congiuntamente da:

a) il presente MDPA;

b) tutti i "DPA - Condizioni Speciali" applicabili in base ai servizi inclusi nell'Ordine (Offerta) sottoscritto dal Titolare, pubblicati e aggiornati agli indirizzi web di cui all'Articolo 1;

c) le funzionalità tecniche e le interfacce dei servizi stessi.

3. PERSONALE AUTORIZZATO E RISERVATEZZA

Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali (dipendenti, collaboratori, amministratori di sistema) si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, e che abbiano ricevuto un'adeguata formazione in materia di protezione dei dati.

COPYRIGHT © DEGG - DIGITAL EVOLUTION FOR A BETTER LIFE | WWW.DEGG.IT

4. SUB-RESPONSABILI (ART. 28, PAR. 2, GDPR)

Con la sottoscrizione del presente accordo, il Titolare fornisce un'autorizzazione generale scritta affinché il Responsabile possa ricorrere a sub-responsabili (Responsabili Ulteriori del Trattamento) per l'esecuzione di specifiche attività di trattamento (es. fornitura di servizi di hosting, cloud computing, assistenza IT).
Il Responsabile informerà il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri sub-responsabili con un preavviso di almeno 15 (quindici) giorni. Il Titolare avrà la facoltà di opporsi a tali modifiche per giustificati motivi legati alla protezione dei dati; in caso di opposizione non superabile, il Titolare potrà recedere dal contratto limitatamente ai servizi impattati. Il Responsabile imporrà ai sub-responsabili i medesimi obblighi in materia di protezione dei dati previsti dal presente MDPA.

5. MISURE DI SICUREZZA (ART. 32 GDPR)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Il dettaglio delle Misure di Sicurezza (tra cui cifratura, controlli di accesso, backup e procedure di incident management) è descritto nell'**Allegato 1** del presente MDPA (MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA). Resta responsabilità esclusiva del Titolare adottare adeguate misure di sicurezza per proteggere le proprie credenziali di autenticazione e i dispositivi utilizzati per accedere ai servizi di DEGG.

6. GESTIONE DELLE VIOLAZIONI DI SICUREZZA (DATA BREACH)

In caso di violazione dei dati personali (Data Breach) che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati affidati dal Titolare, il Responsabile informerà il Titolare senza ingiustificato ritardo dopo esserne venuto a conoscenza. Il Responsabile fornirà, man mano che si rendono disponibili, le informazioni necessarie per consentire al Titolare di ottemperare ai propri obblighi di notifica ex Artt. 33 e 34 del GDPR, e adotterà le misure ragionevoli per mitigare gli effetti della violazione. Resta inteso che la notifica di una violazione non costituisce ammissione di responsabilità da parte di DEGG.

7. TRASFERIMENTO DI DATI EXTRA-UE (CAPO V GDPR)

Qualora il trattamento richieda il trasferimento di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE) privi di una Decisione di Adeguatezza della Commissione Europea, il Responsabile garantisce che tale trasferimento avverrà esclusivamente previa adozione di garanzie adeguate, conferendo fin d'ora mandato a DEGG per la sottoscrizione, ove necessario, delle Clausole Contrattuali Tipo (SCC - Standard Contractual Clauses) approvate dalla Commissione Europea con i sub-responsabili importatori.

8. ASSISTENZA AL TITOLARE E DIRITTI DEGLI INTERESSATI

Tenendo conto della natura del trattamento, il Responsabile assiste il Titolare, nella misura del possibile, con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste di esercizio dei diritti degli interessati (Artt. 15-22 GDPR). Il Responsabile assiste inoltre il Titolare nel garantire il rispetto degli obblighi relativi alla valutazione d'impatto sulla protezione dei dati (DPIA) e alla consultazione preventiva. Eventuali attività di assistenza personalizzata che esulino dalla fornitura standard del servizio potranno essere soggette a specifica tariffazione.

9. DIRITTO DI AUDIT E ISPEZIONE

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'Art. 28 del GDPR. Il diritto di audit del Titolare sarà esercitato, in via prioritaria, tramite la richiesta e la verifica dei Report e delle certificazioni prodotte da revisori indipendenti incaricati da DEGG.

Qualora il Titolare richieda ispezioni dirette, queste dovranno essere concordate per iscritto con un congruo preavviso, non dovranno intralciare la normale operatività aziendale del Responsabile e i relativi costi organizzativi saranno interamente a carico del Titolare.

10. RESTITUZIONE E CANCELLAZIONE DEI DATI

Alla cessazione della fornitura dei servizi, a scelta del Titolare, il Responsabile cancellerà o restituirà tutti i dati personali, provvedendo a distruggere le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati. Come stabilito nelle Condizioni Generali, in assenza di diversa indicazione, il Responsabile manterrà i dati a disposizione per l'estrazione per un periodo transitorio, decorso il quale procederà alla cancellazione definitiva.

11. LIMITAZIONE DI RESPONSABILITÀ

Le Parti concordano espressamente che la responsabilità del Responsabile derivante dal presente MDPA e dalle violazioni della normativa in materia di protezione dei dati personali è soggetta alle medesime limitazioni economiche (c.d. Liability Cap) ed esclusioni per danni indiretti pattuite tra le Parti nel contratto principale (Master Services Agreement o Master SaaS Agreement) che disciplina la fornitura dei servizi.

12 - AGGIORNAMENTO DEI DPA - CONDIZIONI SPECIALI E DEI LINK

Il Responsabile si riserva il diritto di aggiornare unilateralmente i "DPA - Condizioni Speciali" accessibili tramite i link di cui all'Articolo 1 (inclusi, a titolo esemplificativo, l'aggiornamento dell'elenco dei Sub-Responsabili o delle Misure di Sicurezza). In caso di modifiche sostanziali che impattino negativamente sulle garanzie di protezione dei dati, il Responsabile ne darà comunicazione al Titolare con un preavviso di almeno 15 (quindici) giorni, in analogia a quanto previsto dall'Articolo 4 del presente MDPA per la sostituzione dei Sub-Responsabili. La prosecuzione nell'utilizzo dei servizi da parte del Titolare, decorso tale termine senza che sia stata esercitata formale opposizione, equivarrà ad accettazione incondizionata delle nuove Condizioni Speciali pubblicate online. Ai fini probatori, il Responsabile manterrà un archivio digitale delle versioni storiche dei documenti ("Versioning").

ALLEGATO 1 - MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA (ex Art. 32 GDPR)

Il presente Allegato descrive le misure tecniche e organizzative adottate da DEGG S.r.l. (di seguito "Responsabile") per garantire un livello di sicurezza adeguato al rischio, al fine di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. Il Responsabile si riserva la facoltà di aggiornare e modificare tali misure per adeguarle all'evoluzione tecnologica, a condizione che tali modifiche non comportino una riduzione del livello di sicurezza complessivo dei Servizi.

A. MISURE ORGANIZZATIVE

- **Policy e Disciplinari:** Applicazione di dettagliate policy aziendali a cui tutto il personale con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati.
- **Autorizzazione e Gestione Accessi Logici (Least Privilege):** Definizione dei profili di accesso strettamente limitati alle mansioni assegnate e configurati per consentire l'accesso ai soli dati necessari per le operazioni di trattamento. I profili sono soggetti a revisione e controllo periodico.
- **Gestione Interventi di Assistenza:** Regolamentazione stringente degli interventi di supporto per garantire l'esecuzione delle sole attività previste contrattualmente, impedendo trattamenti eccessivi o non autorizzati di dati di titolarità del Cliente.
- **Valutazione d'Impatto (DPIA):** Adozione di una metodologia proprietaria (basata sulle linee guida europee WP248) per l'analisi e la valutazione preventiva dei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati.
- **Gestione Incidenti e Data Breach:** Implementazione di una procedura di Incident Management per il rapido ripristino delle operazioni e di una specifica procedura di Data Breach Response che definisce ruoli, rilevazione, azioni di contrasto, contenimento e modalità di notifica al Cliente.
- **Formazione del Personale:** Erogazione periodica di corsi di formazione sulla corretta gestione e protezione dei dati personali per tutti i dipendenti coinvolti nelle attività di trattamento.

B. MISURE TECNICHE

- **Protezione Perimetrale (Firewall e IDPS):** Protezione dei sistemi contro il rischio di intrusione abusiva (Art. 615-quinquies c.p.) mediante sistemi Intrusion Detection & Prevention e architetture Firewall, costantemente aggiornati.
- **Sicurezza delle Comunicazioni e Antimalware:** Adozione di protocolli di comunicazione sicuri e cifrati in base alle migliori tecnologie disponibili. I sistemi sono difesi dall'azione di software malevoli tramite strumenti antivirus e antimalware sottoposti ad aggiornamento periodico e costante.
- **Autenticazione e Gestione Credenziali:** Accesso ai sistemi consentito unicamente tramite credenziali univoche e personali. Le parole chiave (password) sono gestite conformemente alle best practice di settore (obbligo di modifica al primo accesso, regole di complessità, lunghezza minima, valutazione di robustezza e scadenza periodica).
- **Tracciamento (Logging):** Configurazione dei sistemi per il tracciamento logico degli accessi e delle attività svolte dalle diverse tipologie di utenze (inclusi gli Amministratori), con protezione dei file di log per garantirne la totale integrità.

- **Amministratori di Sistema:** Tenuta di un elenco aggiornato del personale con funzioni di Amministratore di Sistema, formalmente nominato. Implementazione di un sistema di Log Management inalterabile per il tracciamento puntuale delle attività privilegiate, sottoposto a verifiche periodiche di conformità.
- **Business Continuity e Disaster Recovery (Backup):** Adozione di idonee procedure di Backup & Restore per garantire il ripristino tempestivo dell'accesso ai dati in caso di incidenti. Per i servizi che lo prevedono, è attivo un piano di continuità operativa per assicurare la disponibilità dei sistemi anche a fronte di eventi avversi.
- **Vulnerability Assessment & Penetration Test (VAPT):** Esecuzione periodica di analisi delle vulnerabilità e Penetration Test su infrastrutture e applicativi per rilevare e mitigare eventuali esposizioni, simulando scenari di attacco al fine di valutare la tenuta dei meccanismi di sicurezza logica.

C. INFRASTRUTTURA FISICA (DATA CENTER) E SUB-FORNITORI

- **Sicurezza Fisica:** L'accesso fisico alle sale macchine dei Data Center è strettamente controllato e limitato al solo personale autorizzato.
- **Data Center:** Per i servizi erogati tramite l'infrastruttura Hetzner (Germania), le misure di sicurezza fisiche, ambientali e infrastrutturali adottate dal fornitore sono descritte e rese disponibili dal medesimo sul proprio sito istituzionale.