ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI - DATA PROCESSING AGREEMENT

(ex art. 28 del Regolamento UE 2016/679 ed ex D. Lgs. 196/03 come modificato da D. Lgs. 101/18)

Il presente accordo per la protezione di dati personali è concluso tra Ecloga Italia S.p.A., con sede legale in Viale Beatrice d'Este 24, 20122 Milano, P.IVA 03782720969 (di seguito "il Fornitore" o "Ecloga")

E

il soggetto indicato nel Contratto quale cliente (di seguito il "Cliente"), di seguito, congiuntamente, le "Parti" o disgiuntamente la "Parte".

PREMESSO CHE

a) il Cliente ha sottoscritto uno o più contratti con il Fornitore (di seguito il "Contratto");

b) le Parti intendono disciplinare nel presente "accordo per il trattamento dei dati personali - Data Processing Agreement" (nel seguito "DPA" o "Accordo") le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi e le responsabilità connesse al trattamento medesimo, ivi incluso l'impegno assunto dal Fornitore quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679 del 27 aprile 2016 (nel seguito "GDPR");

c) il presente Accordo si applica ai Servizi che comportano il trattamento di Dati Personali per conto del Cliente, descritti nell'Allegato A, ed è parte integrante del Contratto che lo richiama;

Tutto quanto sopra premesso le Parti convengono quanto segue:

1. DEFINIZIONI E INTERPRETAZIONE

1.1. Le premesse costituiscono parte integrante del presente Accordo. Nell'Accordo i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:

1.1.1. "Data di Decorrenza dell'Accordo" indica la data in cui il Cliente sottoscrive il Contratto che richiama il presente Accordo o, se sottoscritto separatamente, il presente Accordo;

1.1.2. "Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente in relazione alla fruizione dei Servizi, nella misura in cui siano oggetto di trattamento da parte del Fornitore per conto del Cliente, sulla base del Contratto;

1.1.3. "Decisione di Adeguatezza" indica una decisione della Commissione Europea sulla base dell'Articolo 45(3) del GDPR in merito al fatto che le leggi di un certo paese garantiscano un adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali;

1.1.4. "Email di notifica" si intende l'indirizzo (o gli indirizzi) email fornito/i dal Cliente, all'atto della sottoscrizione del Servizio o fornito tramite altro canale ufficiale al Fornitore, a cui il Cliente intende ricevere le notifiche da parte del Fornitore;

1.1.5. "Istruzioni" indica le istruzioni scritte impartite dal Titolare nel presente Accordo, incluse le schede dell'Allegato A, e, eventualmente, nel Contratto e nelle variazioni concordate per iscritto ai sensi del punto 3.3;

1.1.6. "Legislazione in materia di Protezione dei Dati Personali" indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia in materia di protezione dei Dati Personali, nonché ogni provvedimento vincolante che

risulti emanato dalle autorità di controllo competenti in materia di protezione dei Dati Personali (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante;

1.1.7. "Personale del Fornitore" indica i dipendenti, i collaboratori e gli altri soggetti che operano sotto l'autorità del Fornitore, designati ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies D. Lgs. 196/2003, con esclusione del personale dei Responsabili Ulteriori del Trattamento;

1.1.8. "Medico Competente" indica il medico nominato dal Cliente ai sensi del D. Lgs. 81/2008, titolare autonomo dei dati relativi alla salute trattati nella sorveglianza sanitaria, per conto del quale il Fornitore opera in forza di distinto accordo ai sensi dell'art. 28 GDPR;

1.1.9. "Richiesta" indica una richiesta di accesso di un Interessato, una richiesta di cancellazione o correzione dei Dati Personali, o una richiesta di esercizio di uno degli altri diritti previsti dal GDPR;

1.1.10. "Responsabile Ulteriore del Trattamento" indica ogni altro responsabile del trattamento (sub-responsabile) di cui il Fornitore si avvalga, ai sensi dell'art. 28 GDPR, per l'esecuzione di specifiche attività di trattamento di Dati Personali per conto del Cliente;

1.1.11. "Servizio/i" indica il servizio o i servizi oggetto dei Contratti sottoscritti tempo per tempo tra il Cliente e il Fornitore che comportano il trattamento di Dati Personali per conto del Cliente, descritti nell'Allegato A;

1.1.12. "Allegato A" indica le schede dei trattamenti per Servizio, che ne specificano oggetto, durata, natura e finalità, tipo di Dati Personali e categorie di interessati ai sensi dell'art. 28, par. 3, GDPR, nonché le eventuali istruzioni specifiche del Servizio;

1.1.13. "Allegato B" indica l'elenco dei Responsabili Ulteriori del Trattamento, la cui versione aggiornata è pubblicata all'indirizzo https://www.eclogaitalia.it/privacy-center/;

1.1.14. "Violazione della Sicurezza dei Dati Personali" indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali occorsa su sistemi gestiti dal Fornitore o comunque sui quali il Fornitore abbia un controllo.

1.2. I termini "ivi compreso/a/i/e" e "incluso/a/i/e" saranno interpretati come se fossero seguiti dall'espressione "a titolo puramente esemplificativo", così da fornire un elenco non esaustivo di esempi.

1.3. Per le finalità del presente Accordo, i termini "Interessato", "Trattamento", "Titolare del trattamento", "Responsabile del trattamento", "Trasferimento" e "Misure tecnico organizzative adeguate" saranno interpretati in conformità alla Legislazione in materia di Protezione dei Dati Personali applicabile.

2. RUOLO DELLE PARTI

2.1. Le Parti riconoscono e convengono che il Fornitore agisce quale Responsabile del trattamento:

a) per conto del Cliente, ai sensi dell'art. 28 del GDPR, per i trattamenti descritti nell'Allegato A relativi ai Servizi oggetto del Contratto, ivi inclusa la gestione dei dati nell'ambito della pianificazione ed erogazione dei servizi;

b) per conto del Medico Competente, per i trattamenti di dati relativi alla salute connessi alla sorveglianza sanitaria, in forza di distinto accordo ai sensi dell'art. 28 GDPR, che non è disciplinato dal presente Accordo salvo quanto previsto nell'Allegato A per la custodia della documentazione sanitaria per conto del Cliente;

2.2. Le parti riconoscono che il Cliente agisce quale Titolare del trattamento dei Dati Personali. Restano esclusi dal presente Accordo i trattamenti che il Fornitore effettua quale titolare autonomo, tra cui l'erogazione della formazione quale soggetto formatore, la gestione del rapporto contrattuale con il Cliente e la conservazione della documentazione degli incarichi di cui al punto 12.1.5, nonché

l'attività di Responsabile della protezione dei dati, ove affidata al Fornitore, disciplinata dal relativo contratto.

2.3. Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.

2.4. Il Fornitore ha nominato un Responsabile della protezione dei dati (DPO), domiciliato presso la sede operativa di Ecloga Italia S.p.A., in via Brescia 23, 20063 Cernusco sul Naviglio (MI), che può essere contattato al seguente indirizzo: rpd@consulentiecloga.it o al numero 02/92143355.

3. TRATTAMENTO DEI DATI PERSONALI

3.1. Con la stipulazione del presente Accordo, il Cliente affida al Fornitore l'incarico di trattare i Dati Personali ai fini della prestazione dei Servizi, così come descritto, per ciascun Servizio, nell'Allegato A e nel Contratto.

3.2. Il Fornitore tratta i Dati Personali soltanto su Istruzione documentata del Cliente, anche in caso di trasferimento verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto; in tal caso informa il Cliente circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

3.3. Il Fornitore si impegna a conformarsi alle Istruzioni, fermo restando che, qualora il Cliente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Cliente le predette variazioni ed i costi connessi.

3.4. Nei casi di cui al punto 3.3 e in caso di richieste del Cliente che comportino il trattamento di Dati Personali che siano, ad avviso del Fornitore, in violazione della Legislazione in materia di Protezione dei Dati Personali, il Fornitore è autorizzato ad astenersi dall'eseguire tali Istruzioni e ne informerà immediatamente il Cliente. In tali casi il Cliente potrà valutare eventuali variazioni alle Istruzioni impartite o contattare l'Autorità di controllo per verificare la liceità delle richieste avanzate.

4. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

4.1. Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi, il Fornitore si impegna a eseguire il trattamento dei Dati Personali:

4.1.1. soltanto nella misura e con le modalità necessarie per erogare i Servizi o per adempiere opportunamente i propri obblighi, previsti dal Contratto e dal presente Accordo ovvero imposti dalla legge o da un organo di vigilanza o controllo competente. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all'Email di notifica;

4.1.2. in conformità alle Istruzioni del Cliente.

4.1.3. nel rispetto delle istruzioni specifiche previste per ciascun Servizio nell'Allegato A.

4.2. Il Personale del Fornitore che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al trattamento dei dati personali. Tale personale è altresì vincolato da obblighi di riservatezza e dal Codice di condotta aziendale e deve attenersi alle policy di riservatezza e di protezione dei dati personali adottate dal Fornitore. Il Personale del Fornitore che tratta dati relativi alla salute è soggetto al segreto professionale o a un obbligo di riservatezza equivalente (art. 9, par. 3, GDPR).

5. AFFIDAMENTO A TERZI

5.1. In relazione all'affidamento a Responsabili Ulteriori del Trattamento di operazioni di trattamento di Dati Personali, le Parti convengono quanto segue:

5.1.1. il Cliente rilascia al Fornitore autorizzazione scritta generale, ai sensi dell'art. 28, par. 2, GDPR, ad affidare operazioni di trattamento di Dati Personali ai Responsabili Ulteriori del Trattamento indicati nell'Allegato B, per i Servizi ivi indicati;

5.1.2. Il Cliente acconsente altresì all'affidamento di operazioni di Trattamento dei Dati Personali a ulteriori soggetti terzi secondo le modalità previste al successivo punto 5.1.3.

5.1.3. Nei casi in cui il Fornitore ricorra a Responsabili Ulteriori del Trattamento per l'esecuzione di specifiche attività di trattamento dei Dati Personali, il Fornitore:

5.1.3.1. si impegna ad avvalersi di Responsabili Ulteriori del Trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, impone loro, mediante contratto, i medesimi obblighi in materia di protezione dei dati previsti dal presente Accordo e garantisce che l'accesso ai Dati Personali, e il relativo trattamento, sarà effettuato esclusivamente nei limiti di quanto necessario per l'erogazione dei servizi affidati; il Fornitore risponde nei confronti del Cliente dell'adempimento degli obblighi dei Responsabili Ulteriori del Trattamento nei soli termini previsti dall'art. 28, par. 4, GDPR, entro i limiti di cui al punto 13.2 e fermo il diritto di rivalsa del Fornitore nei confronti del Responsabile Ulteriore inadempiente;

5.1.3.2. almeno 15 (quindici) giorni prima della data di avvio delle operazioni di trattamento dei Dati Personali da parte del Responsabile Ulteriore del Trattamento informa il Cliente dell'affidamento al terzo (nonché dei dati identificativi) mediante invio di Email di notifica e aggiornamento dell'Allegato B. Entro 15 (quindici) giorni dal ricevimento della comunicazione il Cliente potrà opporsi per iscritto, per motivi ragionevoli attinenti alla protezione dei dati; in mancanza di accordo, il Cliente potrà recedere dal Contratto, fermo restando l'obbligo di corrispondere al Fornitore gli importi dovuti alla data di cessazione del Contratto.

5.1.4. Informazioni aggiuntive sull'elenco dei Responsabili Ulteriori del Trattamento, dei trattamenti loro affidati e della loro ubicazione, sono contenute nell'Allegato B.

6. DISPOSIZIONI IN MATERIA DI SICUREZZA

6.1. Nell'eseguire il trattamento dei Dati Personali, ai fini della prestazione dei Servizi, il Fornitore si impegna ad adottare misure tecnico-organizzative adeguate per evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata di, o l'accesso ai, Dati Personali.

6.1.1. Il Cliente riconosce e accetta che il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni disponibili al Fornitore stesso, presterà assistenza al Cliente nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32-34 del GDPR nei modi seguenti:

6.1.1.1. implementando e mantenendo adeguate misure di sicurezza;

6.1.1.2. conformandosi agli obblighi di cui al punto 6.3.

6.2. Fermi restando gli obblighi di cui al precedente punto 6.1 in capo al Fornitore, il Cliente riconosce e accetta che, nella fruizione dei Servizi, rimane responsabilità esclusiva del Cliente l'adozione di adeguate misure di sicurezza in relazione alla fruizione dei Servizi da parte del proprio personale e di coloro che sono autorizzati ad accedere a detti Servizi.

6.2.1. A tal fine il Cliente si impegna ad utilizzare i Servizi e le funzionalità di trattamento dei Dati Personali in modo da garantire un livello di protezione adeguato al rischio effettivo.

6.2.2. Il Cliente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Cliente o dagli utenti da esso autorizzati per accedere ai Servizi, e per effettuare, presso i propri sistemi, i salvataggi e backup dei Dati Personali al fine di garantire il ripristino dei Dati Personali nel rispetto delle norme di legge.

6.3. Qualora il Fornitore venga a conoscenza di una Violazione di Sicurezza dei Dati Personali, lo stesso:

6.3.1. informerà il Cliente senza ingiustificato ritardo, e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, mediante comunicazione inoltrata all'Email di notifica;

6.3.2. adotterà misure ragionevoli per limitare i possibili danni e ripristinare la sicurezza dei Dati Personali;

6.3.3. fornirà al Cliente, per quanto possibile, una descrizione della Violazione della Sicurezza dei Dati Personali, con le informazioni di cui all'art. 33, par. 3, GDPR disponibili, ivi incluse le misure adottate per evitare o mitigare i potenziali rischi e le attività raccomandate dal Fornitore al Cliente per la gestione della Violazione di Sicurezza;

6.3.4. considererà informazioni confidenziali ai sensi di quanto previsto nel Contratto, le informazioni attinenti alle eventuali Violazioni della Sicurezza, i relativi documenti, comunicati e avvisi e non comunicherà a terzi tali informazioni, fuori dai casi strettamente necessari all'assolvimento degli obblighi del Cliente derivanti dalla Legislazione in materia di Protezione dei Dati Personali senza il previo consenso scritto del Titolare del Trattamento.

6.4. Nei casi di cui al precedente punto 6.3, è responsabilità esclusiva del Cliente adempiere, nei casi previsti dalla Legislazione in materia di Protezione dei Dati Personali, agli obblighi di notificazione della Violazione di Sicurezza all'Autorità di controllo e agli interessati.

6.5. Resta inteso che la notificazione di una Violazione di Sicurezza o l'adozione di misure volte a gestire una Violazione di Sicurezza non costituisce riconoscimento di inadempimento o di responsabilità da parte del Fornitore in relazione a detta Violazione di Sicurezza.

6.6. Il Cliente dovrà comunicare tempestivamente al Fornitore eventuali utilizzi impropri degli account o delle credenziali di autenticazione oppure eventuali Violazioni di Sicurezza di cui abbia avuto conoscenza riguardanti i Servizi.

7. LIMITAZIONI AL TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

7.1. Il Fornitore non trasferirà i Dati Personali al di fuori dello SEE se non in accordo con il Cliente, ivi incluso quanto indicato nell'Allegato B, e nel rispetto del Capo V del GDPR. È consentito il trasferimento verso paesi o destinatari che beneficiano di una Decisione di Adeguatezza, incluso l'EU-US Data Privacy Framework per i destinatari certificati.

7.2. Se, ai fini della conservazione o del trattamento dei Dati Personali da parte di un Responsabile Ulteriore del trattamento, è necessario effettuare il trasferimento dei Dati Personali fuori dallo SEE in un paese che non gode di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, il Fornitore:

7.2.1. stipulerà, quale esportatore, con il Responsabile Ulteriore del trattamento le clausole contrattuali tipo adottate dalla Commissione europea con Decisione di esecuzione (UE) 2021/914 del 4 giugno 2021, modulo tre (da responsabile a responsabile) (le “Clausole Contrattuali Tipo”), o quelle che dovessero sostituirle, anche mediante le condizioni contrattuali di quest'ultimo. Copia delle Clausole Contrattuali Tipo sarà resa disponibile al Cliente su richiesta; e/o

7.2.2. potrà proporre al Cliente altre garanzie adeguate previste dagli artt. 46 e 47 GDPR, quali le norme vincolanti d'impresa approvate per il gruppo cui appartiene il Responsabile Ulteriore del Trattamento.

8. VERIFICHE E CONTROLLI

8.1. Il Fornitore verifica periodicamente l'efficacia delle misure di sicurezza dei sistemi dallo stesso utilizzati per l'erogazione dei Servizi e delle sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report

("Report"). Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.

8.2. Ove siano disponibili Report ai sensi del punto 8.1, il Cliente concorda di esercitare il proprio diritto di verifica in primo luogo mediante l'esame dei Report e delle informazioni messe a disposizione dal Fornitore, fermo restando quanto previsto al punto 8.3.

8.3. Il Fornitore riconosce il diritto del Cliente, con le modalità e nei limiti di seguito indicati, ad effettuare audit indipendenti per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo e di quanto previsto dalla normativa. Il Cliente potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.

8.4. Nel caso di cui al precedente punto 8.3, il Cliente dovrà previamente inviare richiesta scritta al Responsabile della Protezione dei Dati (DPO) del Fornitore. Successivamente alla richiesta di audit o ispezione il Fornitore e il Cliente concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il Cliente e coloro che effettuano le verifiche e i costi che il Fornitore potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.

8.5. Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che siano, sulla base di motivate ragioni, non adeguatamente qualificati o indipendenti, siano concorrenti del Fornitore o che siano evidentemente inadeguati. In tali circostanze il Cliente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

8.6. Il Cliente si impegna a corrispondere al Fornitore gli eventuali costi calcolati dal Fornitore e comunicati al Cliente nella fase di cui al precedente punto 8.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.

8.7. Resta fermo quanto previsto in relazione ai diritti di ispezione del Titolare del trattamento e delle autorità nelle Clausole Contrattuali Tipo eventualmente sottoscritte ai sensi del precedente punto 7, che non potranno considerarsi modificate da alcuna delle previsioni contenute nel presente Accordo.

8.8. Le attività di verifica che interessino eventuali Responsabili Ulteriori dovranno essere svolte nel rispetto delle regole di accesso e delle politiche di sicurezza dei Responsabili Ulteriori.

9. ASSISTENZA A FINI DI CONFORMITÀ

9.1. Il Fornitore presterà assistenza al Cliente e coopererà nei modi di seguito indicati al fine di consentire al Cliente il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.

9.2. Qualora il Fornitore riceva Richieste o reclami da un Interessato in relazione ai Dati Personali, il Fornitore raccomanderà all'Interessato di rivolgersi al Cliente, nel caso in cui quest'ultimo sia il Titolare del Trattamento, senza darvi riscontro diretto salvo diversa Istruzione del Cliente. In tali casi il Fornitore informerà tempestivamente il Cliente del ricevimento della Richiesta mediante invio di Email di notifica e fornirà al Cliente le informazioni ad esso disponibili unitamente a copia della Richiesta o del reclamo. Resta inteso che, salvo che il supporto nella gestione delle Richieste sia oggetto del Servizio secondo l'Allegato A, tale attività di cooperazione sarà svolta in via eccezionale, in quanto la gestione dei rapporti con gli Interessati resta esclusa dai Servizi ed è responsabilità del Cliente gestire eventuali reclami in via diretta e garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il Cliente stesso. Sarà responsabilità del Cliente provvedere a dar seguito a tali Richieste o reclami.

9.3. Il Fornitore provvederà a informare tempestivamente il Cliente, salvo il caso in cui ciò sia vietato dalla legge, con avviso all'Email di notifica di eventuali ispezioni o richieste di informazioni presentate da autorità di controllo e forze di polizia rispetto a profili che riguardano il trattamento dei Dati Personali.

9.4. Qualora, ai fini dell'evasione delle Richieste di cui ai precedenti punti, il Cliente abbia necessità di ricevere informazioni dal Fornitore circa il trattamento dei Dati Personali, il Fornitore presterà la necessaria assistenza nei limiti di quanto ragionevolmente possibile, a condizione che tali richieste siano presentate con congruo preavviso.

9.5. Il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili, fornirà ragionevole assistenza al Cliente nel rendere disponibili informazioni utili per consentire al Cliente l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali e per l'eventuale consultazione preventiva dell'Autorità di controllo, nei casi previsti dagli artt. 35 e 36 GDPR. In tal caso il Fornitore renderà disponibili informazioni di carattere generale in base al Servizio, quali le informazioni contenute nel Contratto e nel presente Accordo. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del Cliente. Resta inteso che è responsabilità e onere esclusivo del Cliente procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei Dati Personali dallo stesso posto in essere nel contesto dei Servizi.

9.6. Il Fornitore si impegna a rendere Servizi improntati ai principi di minimizzazione del trattamento (privacy by design & by default), fermo restando che è responsabilità esclusiva del Cliente assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi e verificare che le misure tecniche e organizzative di un Servizio soddisfano i requisiti di conformità del Cliente, ivi inclusi i requisiti previsti dalla Legislazione in materia di protezione dei dati personali.

9.7. Il Cliente prende atto che, in caso di Richieste di portabilità dei Dati Personali avanzate dai rispettivi Interessati, e solo in relazione ai Servizi che generano Dati Personali rilevanti a tal fine, il Fornitore presterà assistenza al Cliente mettendo a disposizione le informazioni necessarie per estrarre i dati richiesti in formato conforme a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.

10. OBBLIGHI DEL CLIENTE E LIMITAZIONI

10.1. Il Cliente si impegna a impartire Istruzioni conformi alla normativa.

10.2. Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento dalla Legislazione in materia di Protezione dei Dati Personali, ivi inclusi gli obblighi di informativa nei confronti degli Interessati.

10.3. È altresì onere esclusivo del Cliente provvedere alla gestione dei Dati Personali in conformità alle Richieste avanzate dagli Interessati, e pertanto provvedere ad esempio agli eventuali aggiornamenti, integrazioni, comunicazioni di rettifiche e cancellazioni dei Dati Personali.

10.4. È onere del Cliente mantenere l'account collegato all'Email di notifica attivo ed aggiornato.

10.5. Il Cliente prende atto che, ai sensi dell'art. 30 del GDPR, il Fornitore è tenuto a mantenere un registro delle attività di trattamento eseguite per conto dei Titolari del Trattamento e a raccogliere a tal fine i dati identificativi di ciascun Titolare (e/o Responsabile) del Trattamento per conto del quale il Fornitore agisce e che tali informazioni devono essere rese disponibili all'autorità competente, su richiesta. Pertanto, quando richiesto, il Cliente si impegna a dare al Fornitore i dati identificativi sopra indicati con le modalità individuate dal Fornitore nel tempo e a mantenere aggiornate tali informazioni tramite i medesimi canali.

11. DURATA

11.1. Il presente Accordo avrà efficacia a decorrere dalla Data di Decorrenza dell'Accordo e cesserà automaticamente, alla data di cancellazione di tutti i Dati Personali da parte del Fornitore, come previsto nel presente Accordo.

12. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONE DEI DATI PERSONALI

12.1. Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore cesserà ogni trattamento dei Dati Personali per conto del Cliente e, salvo quanto previsto ai punti 12.1.4 e 12.1.5:

12.1.1. provvederà alla cancellazione dei Dati Personali (ivi incluse eventuali copie) dai sistemi del Fornitore o da quelli su cui lo stesso abbia controllo decorso il periodo di cui al punto 12.1.3, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria al fine di assolvere ad una disposizione di legge italiana o europea;

12.1.2. distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria ai fini del rispetto di norme di legge italiane o europee; e

12.1.3. manterrà a disposizione del Cliente i Dati Personali per l'estrazione per il periodo di 12 (dodici) mesi successivi alla cessazione del Contratto. Durante tale periodo, il trattamento sarà limitato alla sola conservazione finalizzata a mantenere i Dati Personali a disposizione del Cliente per l'estrazione di cui al punto 12.2.

12.1.4. per la documentazione sanitaria custodita per conto del Cliente alla cessazione dell'incarico del Medico Competente (art. 25, co. 1, lett. d) ed e), D. Lgs. 81/2008), la consegnerà al Cliente o, su sua istruzione, al nuovo medico competente da questi nominato; in mancanza di istruzioni ne proseguirà la custodia per il periodo di conservazione previsto dalla legge, al termine del quale provvederà alla cancellazione definitiva;

12.1.5. resta salva la conservazione, da parte del Fornitore quale titolare autonomo, della documentazione prodotta nell'esecuzione degli incarichi di consulenza in materia di salute e sicurezza sul lavoro, limitata a quanto necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, per 10 anni dalla cessazione dell'incarico e, in presenza di contestazioni o procedimenti, fino alla loro definizione.

12.2. Fermo restando quanto altrimenti previsto nel presente Accordo, il Cliente riconosce di poter estrarre i Dati Personali, alla cessazione del Servizio, nei modi convenuti e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto 12.1.3.

13. RESPONSABILITA'

13.1. Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente Accordo e dalla Legislazione in materia di protezione dei Dati Personali.

13.2. Fatti salvi i limiti inderogabili di legge, il Fornitore sarà tenuto a risarcire il Cliente in caso di violazione del presente Accordo entro i limiti massimi convenuti nel Contratto.

14. DISPOSIZIONI VARIE

14.1. Il presente Accordo sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsivoglia istruzione fornita in qualsiasi forma dal Cliente al Fornitore precedentemente alla data del presente Accordo in merito ai Dati Personali trattati nell'ambito dell'esecuzione del Contratto.

14.2. Il presente Accordo potrà essere modificato dal Fornitore dandone comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Cliente e pubblicando la nuova versione all'indirizzo indicato nel Contratto. In tal caso, il Cliente avrà il diritto di recedere dal Contratto con

comunicazione scritta inviata al Fornitore a mezzo raccomandata con ricevuta di ricevimento nel termine di 15 giorni dal ricevimento della comunicazione del Fornitore. In mancanza di esercizio del diritto di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al presente Accordo si intenderanno da questi definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

14.3. In caso di conflitto tra le previsioni del presente Accordo e quanto previsto nel Contratto per la prestazione dei Servizi, o in documenti del Cliente non espressamente accettati dal Fornitore in deroga al presente Accordo, prevarrà quanto previsto nel presente Accordo. Per ciascun Servizio, le istruzioni specifiche dell'Allegato A prevalgono sulle disposizioni generali del presente Accordo.

14.4. Il presente Accordo, con i relativi allegati, costituisce parte integrante del Contratto che lo richiama e si intende accettato con la sottoscrizione di quest'ultimo; la versione vigente è pubblicata all'indirizzo indicato nel Contratto.

Cernusco sul Naviglio, ____ / ____ / _____

Firma del Responsabile del Trattamento
Ecloga Italia spa
ECLOGA ITALIA S.p.A.
Presidente CdA
Marco Fornara

Firma Cliente Titolare del Trattamento

Ragione Sociale _____

Timbro e Firma _____

Allegato A

Schede dei trattamenti per Servizio

Ciascuna scheda descrive il trattamento svolto per conto del Cliente. Si applicano le schede dei Servizi oggetto del Contratto sottoscritto. Salvo quanto indicato in scheda, i trattamenti hanno la durata del Contratto.

A.1 RSPP esterno e consulenza in materia di salute e sicurezza sul lavoro

Trattamento	Incarico di RSPP esterno e consulenza connessa. Sopralluoghi, valutazione dei rischi, anche con fotografie e video delle postazioni, redazione del DVR e degli altri documenti. Messa a disposizione nell'Area Clienti degli elaborati prodotti.
Natura	Raccolta, registrazione, consultazione, elaborazione, conservazione, messa a disposizione nell'Area Clienti, cancellazione.
Finalità	Adempimento degli obblighi del Cliente ai sensi del D. Lgs. 81/2008.
Tipo di dati personali	Dati anagrafici e di contatto; mansione e reparto; immagini dei lavoratori eventualmente ripresi nelle fotografie e nei video delle postazioni.
Categorie di interessati	Lavoratori e referenti del Cliente.
Istruzioni specifiche	Fotografie e video sono acquisiti per la sola valutazione dei rischi, limitando per quanto possibile la riconoscibilità dei lavoratori, e non sono utilizzati per il controllo della loro attività. Alla cessazione dell'incarico si applica il punto 12.1.5.

A.2 Consulenza sui sistemi di gestione

Trattamento	Predisposizione e mantenimento della documentazione del sistema di gestione, audit interni, supporto nelle verifiche dell'ente di certificazione.
Natura	Raccolta, registrazione, consultazione, elaborazione, conservazione, cancellazione.
Finalità	Attuazione e mantenimento del sistema di gestione del Cliente.
Tipo di dati personali	Dati anagrafici e di contatto; ruolo e mansione; registrazioni del sistema di gestione (competenze, formazione, esiti degli audit).
Categorie di interessati	Lavoratori, collaboratori e referenti del Cliente.

A.3 Consulenza in materia di protezione dei dati personali

Trattamento	Redazione e aggiornamento dell'impianto documentale; supporto nella gestione delle violazioni dei dati personali e delle richieste degli interessati.
Natura	Raccolta, consultazione, elaborazione, conservazione, cancellazione.
Finalità	Supporto al Cliente nell'adempimento degli obblighi previsti dal GDPR.
Tipo di dati personali	Dati anagrafici e di contatto; ruoli e mansioni; dati relativi agli eventi di violazione e alle richieste degli interessati, anche di categorie particolari o relativi a reati (artt. 9 e 10 GDPR), nei limiti strettamente necessari all'incarico.
Categorie di interessati	Lavoratori, collaboratori, clienti, fornitori e altri interessati del Cliente, nei limiti dei dati necessari all'incarico.
Istruzioni specifiche	Il supporto nella gestione delle Richieste rientra nel Servizio; il riscontro all'interessato resta in capo al Cliente. L'attività di Responsabile della protezione dei dati, ove affidata, è disciplinata dal relativo contratto.

A.4 Gestione organizzativa della medicina del lavoro per conto del datore di lavoro

Trattamento	Organizzazione della sorveglianza sanitaria, gestione anagrafiche lavoratori, pianificazione delle visite, invio di promemoria anche via SMS, gestione dello scadenziario; trasmissione dei giudizi di idoneità al Cliente; custodia della documentazione sanitaria alla cessazione dell'incarico del Medico Competente.
Natura	Raccolta, registrazione, organizzazione, consultazione, conservazione, comunicazione al Cliente e al Medico Competente, invio di promemoria, custodia, cancellazione.
Finalità	Adempimento degli obblighi del Cliente in materia di sorveglianza sanitaria (D. Lgs. 81/2008).
Tipo di dati personali	Dati anagrafici e di contatto; mansione e rischi; scadenziario prestazioni mediche; giudizio di idoneità e relative prescrizioni o limitazioni, ove presenti; documentazione sanitaria, nella sola custodia successiva alla cessazione dell'incarico del Medico Competente.
Categorie di interessati	Lavoratori del Cliente soggetti a sorveglianza sanitaria.
Istruzioni specifiche	Il Cliente conviene che la cartella sanitaria e di rischio sia custodita sui sistemi del Fornitore e, alla cessazione dell'incarico del Medico Competente, ne affida al Fornitore la custodia per suo conto, con salvaguardia del segreto professionale e messa a disposizione del nuovo medico competente. Se il Cliente nomina il medico di una struttura sanitaria delegata, la struttura opera quale Responsabile Ulteriore del Trattamento del Fornitore per i soli aspetti organizzativi e al Fornitore è trasmesso il solo giudizio di idoneità.

A.5 Area Clienti e Safety First: gestione delle scadenze e dei documenti in materia di salute e sicurezza

Trattamento	Messa a disposizione dell'Area Clienti, anche come servizio autonomo (Safety First), per gestire scadenze e documenti previsti dal D. Lgs. 81/2008: anagrafica e scadenziario formativo dei lavoratori, anche per corsi di altri enti, scadenze e certificati di idoneità della sorveglianza sanitaria, altri adempimenti, archivio dei documenti.
Natura	Registrazione, conservazione, messa a disposizione del Cliente tramite la piattaforma, backup, cancellazione.
Finalità	Supporto al Cliente nell'adempimento degli obblighi previsti dal D. Lgs. 81/2008.
Tipo di dati personali	Dati anagrafici e di contatto; mansione; corsi frequentati, attestati e relative scadenze; scadenze della sorveglianza sanitaria e certificati di idoneità alla mansione; dati contenuti nei documenti caricati dal Cliente o dal Fornitore.
Categorie di interessati	Lavoratori e referenti del Cliente.

A.6 Piattaforma di segnalazione Whistli

Trattamento	Fornitura in modalità SaaS della piattaforma per la ricezione e la gestione delle segnalazioni del Cliente ai sensi del D. Lgs. 24/2023 e, ove previsto dal Contratto, di ulteriori canali istituiti dal Cliente per le segnalazioni di violenze, abusi e molestie.
Natura	Conservazione, messa a disposizione del Cliente, backup, cancellazione.
Finalità	Gestione del canale interno di segnalazione del Cliente (D. Lgs. 24/2023) e, ove previsto, degli ulteriori canali di segnalazione istituiti dal Cliente.
Tipo di dati personali	Dati identificativi e di contatto del segnalante, ove forniti; contenuto delle segnalazioni, che può includere dati di categorie particolari (art. 9 GDPR), quali dati relativi alla salute o vita sessuale, e dati relativi a reati (art. 10 GDPR).
Categorie di interessati	Segnalanti, segnalati, facilitatori, presunte vittime e altre persone coinvolte o menzionate nelle segnalazioni.
Istruzioni specifiche	Il Fornitore e i Responsabili Ulteriori del Trattamento non accedono al contenuto delle segnalazioni né all'identità dei segnalanti. Il Fornitore mette a disposizione la valutazione d'impatto della piattaforma.

Allegato B

Il Fornitore si avvale dei seguenti Responsabili del Trattamento per i Servizi indicati (numerazione rif. schede Allegato A). La versione aggiornata del presente elenco è pubblicata all'indirizzo eclogaitalia.it/privacy-center/; le modifiche sono comunicate secondo il punto 5.1.3.2. Di seguito l'elenco dei sub-responsabili:

Sub-Responsabile - Ragione sociale	Sede aziendale
Elatos S.r.l. - gestionale e piattaforme (tutti i Servizi)	Desenzano del Garda (BS)
Aruba S.p.A. - datacenter (tutti i Servizi)	Ponte San Pietro (BG)
Google Cloud Italy S.r.l. - Google Workspace (A.1-A.5)	Milano (MI), con dati conservati in UE
Basics s.r.l. - amministrazione dell'infrastruttura informatica (A.1-A.5)	Basiano (MI)
8volante S.r.l. - amministrazione dominio Google Workspace (A.1-A.5)	Orzinuovi (BS)
Openapi S.p.A. - invio notifiche SMS (A.4)	Roma (RM)
Strutture sanitarie delegate - organizzazione delle visite (A.4)	Comunicata al Cliente all'atto dell'affidamento
Anthropic, PBC - strumenti IA, esclusi dati lavoratori e dati relativi alla salute (A.1-A.3)	San Francisco (USA – SCC);