Gruppo Sapio

Contratto per il Trattamento dei Dati Personali Infragruppo

Sapio Produzione Idrogeno Ossigeno S.r.l. – Advice Pharma Group S.r.l.

INFORMAZIONI:

Titolo	Contratto per il Trattamento dei Dati Personali Infragruppo		
Data di emissione	10.11.2022	**Versione**	1.0

PREAMBOLO

Premesso che:

A. I Dati Personali sono Trattati all'interno del Gruppo Sapio ("Gruppo Sapio") da molteplici affiliate, che possono Trattare i Dati Personali autonomamente, per i propri fini, oppure assieme a un'altra affiliata.

B. Quando i Dati Personali sono Trattati da un'affiliata per assistere un'altra affiliata o per fornirle un servizio, i Dati Personali saranno Trattati per conto della seconda affiliata. In questo caso, può dirsi che la prima affiliata tratta Dati Personali per conto della seconda affiliata (vale a dire, per finalità definite da quest'ultima). In tal caso la prima affiliata sarà generalmente considerata, ai sensi delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, come Responsabile, agendo per conto della seconda, che sarà considerata Titolare.

C. I rapporti tra un Titolare e un Responsabile devono essere regolati per mezzo di un accordo scritto, che integri i requisiti minimi stabiliti dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali – anche quando Titolare e Responsabile fanno parte dello stesso Gruppo di Imprese.

D. Inoltre, alcune affiliate potrebbero trasferire Dati Personali al di fuori dal SEE/UE, in paesi che non hanno ricevuto una decisione vincolante emessa dalla Commissione Europea che permette il trasferimento di Dati Personali dal SEE verso un paese terzo il cui ordinamento interno fornisca un adeguato livello di tutela in materia di protezione dei dati personali. Quando ciò accade, devono essere stabilite idonee garanzie al fine di rendere legittimo il trasferimento di Dati Personali, ai sensi delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

E. Questo Contratto per il Trattamento dei Dati Personali Infragruppo, assieme ai suoi Allegati (congiuntamente, il "**CTDPI**"), viene concluso tra Sapio Produzione Idrogeno Ossigeno S.r.l., con sede in via S. Maurilio 13, Milano, P.IVA 10803700151, nella persona del proprio rappresentante legale pro tempore (di seguito "**Sapio**" o il "**Responsabile**") e Advice Pharma S.r.l., con sede legale in Via Arezzo 10/7 20162 Milano MI)., Italia, P. IVA n. IT07674580969 (di seguito l'"**Affiliata**" o "**Titolare**"). Il Titolare e il Responsabile (congiuntamente intesi come le "**Parti**", e ciascuno singolarmente come "**Parte**") riflettendo gli accordi sanciti tra le Parti relativamente al Trattamento di Dati Personali e stabilendo garanzie adeguate per qualsiasi eventuale trasferimento di Dati Personali, in conformità ai requisiti delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

F. Le attività di Trattamento eseguite dal Responsabile, nonché la/le finalità del Trattamento di Dati Personali relative a tali attività di Trattamento, sono meglio specificati nell'Allegato 3.

G. Queste attività di Trattamento di Dati Personali potrebbero essere soggette all'applicazione di Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, che potrebbero stabilire taluni obblighi per i Trattamento di Dati Personali. Le leggi applicabili a queste attività saranno quelle applicabili al Titolare in ciascun caso.

H. Le Parti hanno concluso il presente CTDPI al fine di assicurarsi la conformità alle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali e stabilire misure di sicurezza e procedure idonee per procedere al legittimo Trattamento dei Dati Personali.

Il suddetto preambolo forma parte integrante del presente CTDPI.

DEFINIZIONI

Salvo che sia diversamente definito nel presente CTDPI, tutti i termini in maiuscolo utilizzati nel presente CTDPI hanno il significato loro attribuito nel Contratto Master (come infra definito). In caso di contrasto o incongruenze per quanto riguarda la tutela della protezione dei dati tra il presente CTDPI e il Contratto Master, prevale quanto stabilito nel presente CTDPI;

"Affiliata" indica la società del Gruppo Sapio Titolare del Trattamento. Ai sensi del presente CTDPI, si intende Advice Pharma S.r.l.;

"Autorità di Controllo" indica ogni autorità competente a vigilare ed assicurare l'applicazione delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali con riferimento al Trattamento dei Dati Personali del Titolare svolti nell'ambito del presente CTDPI;

"Categorie Particolari di Dati Personali" indica i Dati Personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il Trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;

"Contratto Master": indica il contratto (o i contratti) disciplinante la fornitura del/i servizio/i concluso tra le Parti;

"CTDPI" indica il presente Contratto per il Trattamento dei Dati Personali Infragruppo, insieme agli Allegati da 1 a 4;

"Dati Personali" significa qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; al fine di evitare contrasti interpretativi,

"Dati Personali**"** ha il significato previsto dal Regolamento e dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali;

"Diritti dell'Interessato" sono i diritti riconosciuti all'Interessato dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali. Nei limiti di applicabilità del Regolamento, "Diritti dell'Interessato" significa, ad esempio, il diritto di chiedere al Titolare l'accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del Trattamento dei dati dell'Interessato o il diritto di opposizione al Trattamento, nonché il diritto alla portabilità dei dati;

"Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali" indica, negli Stati membri dell'Unione Europea, il Regolamento e le complementari legislazioni nazionali in materia di protezione dei

Dati Personali, comprensivi di ogni orientamento e/o *code of pratice* emessi dalla competente Autorità di controllo all'interno dell'Unione Europea; e/o, negli Stati extra UE, ogni vigente legislazione in materia di protezione dei Dati Personali relativa alla tutela ed al legittimo Trattamento di Dati Personali;

"**Elenco dei Sub-Responsabili**" indica l'elenco che potrà essere comunicato ai Titolari su richiesta, come disposto all'Art. 5;

"Entità extra SEE" indica ogni organismo che Tratti Dati Personali nell'ambito delle attività di Trattamento descritte nell'Allegato 3 in un paese extra SEE o in un paese che non abbia ricevuto una decisione vincolante emessa dalla Commissione Europea che permette il trasferimento dei dati dallo SEE verso un paese terzo;

"Esportatore" ha il significato previsto dalle SCCs;

"Importatore" ha il significato previsto dalle SCCs;

"Interessato/i" ha il significato previsto dal Regolamento;

"Meccanismi di Trasferimento": si intende una decisione di adeguatezza vincolante emessa dalla Commissione Europea che permette il trasferimento di Dati Personali dal SEE verso un paese terzo il cui ordinamento interno fornisca un adeguato livello di tutela in materia di protezione dei dati personali. Ove tale decisione vincolante non sia presente o efficace, si intendono le Clausole Contrattuali Tipo (di seguito, "**SCCs**") – qui richiamate per referenza - di volta in volta approvate dalla Commissione Europea per il trasferimento di Dati Personali nonché le norme vincolanti di impresa (BCRs);

"Regolamento" indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE;

"Responsabile" indica generalmente la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che Tratti Dati Personali per conto del Titolare;

"**SEE**" indica lo Spazio Economico Europeo;

"**Sub-Responsabile**" indica un organismo individuato dal Responsabile per assisterlo nel (o che intraprenda direttamente qualsivoglia) trattamento dei Dati Personali per conto del Titolare, nel rispetto delle obbligazioni previste dal Responsabile e di cui al presente CTDPI, individuabile nell'Elenco dei Sub-Responsabili;

"Titolare" indica generalmente la persona fisica o giuridica, la pubblica autorità, l'organismo o altro ente che, da solo o congiuntamente con altri soggetti, determini le finalità e le modalità del Trattamento dei Dati Personali;

"Trattare" o "**Trattamento**" significa qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

"**UE**" indica l'Unione Europea;

"Violazione 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 trasmessi, conservati o comunque trattati.

RUOLI PRIVACY

2.1. Le Parti convengono che:

a) l'Affiliata agisce come Titolare del Trattamento dei Dati Personali posto in essere dal Responsabile nell'ambito delle attività di Trattamento effettuate;
b) Sapio agisce come Responsabile del Trattamento dei Dati Personali nell'ambito delle attività di Trattamento effettuate;
c) il presente CTDPI regola il rapporto tra le Parti con riferimento ai rispettivi compiti e obblighi con riferimento al Trattamento dei Dati Personali posto in essere dal Responsabile nell'ambito del Trattamento dei Dati.

3. OBBLIGHI DEL RESPONSABILE

3.1. Il Titolare determina le finalità del Trattamento dei Dati Personali del Titolare.

3.2. Oltre agli obblighi stabiliti negli Allegati 1 e 2 del presente CTDPI, il Responsabile si impegna a rispettare i seguenti obblighi:

a) Il Responsabile tratterà i Dati Personali del Titolare solo per quanto strettamente necessario, restando soggetto alle istruzioni impartite per iscritto dal Titolare con il presente CTDPI;
b) Il Responsabile avvertirà il Titolare qualora ritenga che le istruzioni impartite per iscritto si pongano in violazione delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.
c) Il Responsabile informerà tempestivamente il Titolare, senza indebito ritardo, di ogni contatto o comunicazione ricevuta da un'Autorità di Controllo in relazione al Trattamento dei Dati Personali del Titolare. A tal riguardo, le Parti acconsentono e concordano che la responsabilità per il riscontro a tali richieste rimarrà esclusivamente in capo al Titolare e non al Responsabile.
d) Il Responsabile ha implementato misure operative, tecniche e organizzative adeguate ai sensi dell'articolo 32 del Regolamento (le quali sono descritte nell'Allegato 2 del presente CTDPI), per proteggere i Dati Personali (comprese le Categorie Particolari di Dati Personali). Il Titolare e il Responsabile sono consapevoli e concordano che il Responsabile è espressamente autorizzato ad implementare misure alternative o stabilire luoghi alternativi di conservazione dei dati purché il livello di sicurezza delle misure o dei luoghi scelti sia ritenuto, sotto tutti gli aspetti, adeguato.
e) Ove il Responsabile comunichi i Dati Personali trattati al proprio personale, il Responsabile assicura che detto personale:
    i) sia impegnato a mantenere la riservatezza o sia soggetto ad un obbligo legale di riservatezza e;
    ii) tratti i Dati Personali del Titolare seguendo le istruzioni del Responsabile nel rispetto degli obblighi contenuti nel presente CTDPI.
f) Il Responsabile è tenuto ad assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.

OBBLIGHI DEL TITOLARE

4.1. Il Titolare è consapevole e accetta che, affinché il Responsabile possa effettuare le attività di Trattamento di Dati Personali stabilite nell'Allegato 3, il Titolare fornirà al Responsabile Dati Personali del Titolare.

4.2. Il Titolare assicura e garantisce che sussiste un'idonea base legale (ad es., consenso dell'Interessato, legittimo interesse, autorizzazione dalla competente Autorità di Controllo ecc.) per procedere al Trattamento e alla trasmissione dei Dati Personali del Titolare al Responsabile.

AUTORIZZAZIONE AL TRATTAMENTO DA PARTE DI SUB-RESPONSABILI

5.1. Il Titolare riconosce, accetta ed acconsente che, nel rispetto di quanto stabilito nel presente CTDPI, i Dati Personali potrebbero essere Trattati dal Responsabile o dai suoi Sub-Responsabili come descritti nell'Elenco dei Sub-Responsabili, di cui all'Allegato 4.

5.2. Ai sensi dell'art. 5.1, il Responsabile è autorizzato a servirsi di Sub-Responsabili a condizione che:

a) fornisca al Titolare, dietro richiesta dello stesso, l'Elenco dei Sub-Responsabili, di cui all'Allegato 4, che include l'identità, il paese di stabilimento e il ruolo assunto da ciascun Sub-Responsabile impiegato;
b) renda disponibile al Titolare ogni aggiornamento del predetto elenco al fine di consentire al Titolare di opporsi all'impiego di detti Sub-Responsabili;
c) stipuli accordi con i Sub-Responsabili che contengano gli stessi obblighi previsti dal presente CTDPI per quanto riguarda il Trattamento dei Dati Personali;
d) eserciti adeguati controlli nel selezionare i Sub-Responsabili e rimanga responsabile per l'adempimento degli obblighi contenuti nel presente CTDPI da parte dei Sub-Responsabili coinvolti;
e) fornisca al Titolare adeguate informazioni in merito alle azioni ed alle misure che il Responsabile ed i suoi Sub-Responsabili hanno intrapreso per assicurare il rispetto delle previsioni del presente CTDPI.

TRASFERIMENTO DEI DATI PERSONALI E INCLUSIONE DELLE CLAUSOLE CONTRATTUALI TIPO

6.1. Le Parti riconoscono e accettano che tutti i trasferimenti transfrontalieri ritenuti strettamente necessari per svolgere efficacemente il Servizio sono autorizzati ai sensi del presente CTDPI e saranno regolati da un Meccanismo di trasferimento applicabile.

6.2. Qualora fosse necessario effettuare trasferimenti transfrontalieri per svolgere efficacemente il servizio e non siano disponibili altri Meccanismi di Trasferimento diversi dalle SCCs, le Parti concordano di stipulare e rispettare le SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento" (che si intendono incorporate nel presente CTDPI per referenza), che sono considerate applicabili a un determinato trasferimento transfrontaliero.

6.3. Se le SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento" sono considerate applicabili ai sensi delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali:

(a) gli Allegati 1- 2 e 4 del presente Contratto si applicheranno e saranno considerati come gli Annex 1-2-3 delle SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento";

(b) l'Esportatore fornirà la sua autorizzazione generale scritta per la nomina di subresponsabili mediante l'Allegato 4 del presente CTDPI. L'Importatore informerà specificamente ogni Importatore di dati di qualsiasi modifica prevista all'Allegato 4 ai sensi della Clausola 5;
(c) le SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento" saranno disciplinate dalla legge di uno degli Stati membri dell'UE, a condizione che tale legge consenta l'esercizio dei diritti dei terzi beneficiari. Le parti concordano che la legge italiana sarà la legge della giurisdizione dell'Esportatore (se l'Esportatore si trova nell'UE) o dell'Importatore (se l'Importatore si trova nell'UE e l'Esportatore no);
(d) qualsiasi controversia derivante dalle SCCs sarà risolta dai tribunali della giurisdizione dell'Esportatore (dove l'Esportatore si trovi nell'UE) o dell'Importatore (dove l'Importatore si trovi nell'UE, e l'Esportatore non lo sia). Nel caso in cui né l'Esportatore né l'Importatore si trovino all'interno dell'UE, saranno competenti i tribunali della giurisdizione dell'Esportatore;
(e) gli Interessati possono anche intentare un'azione legale contro l'Esportatore e/o l'Importatore per la violazione dei loro diritti di terzi beneficiari ai sensi delle SCCs davanti ai tribunali dello Stato membro dell'UE in cui l'Interessato ha la sua residenza abituale o luogo di lavoro. Le Parti accettano di sottoporsi alla giurisdizione di tali tribunali;
(e) il presente CTDPI è considerato un'integrazione non conflittuale delle SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento". In caso di conflitto, le disposizioni delle SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento" prevarranno su quelle del presente CTDPI.
6.4. Ai sensi del Considerando G), le Parti concordano di stipulare ulteriori clausole contrattuali locali di trasferimento locali, qualora ciò sia richiesto dalla legislazione applicabile in materia di protezione dei dati per garantire la legittimità di un determinato trasferimento transfrontaliero.
6.5. In caso di conflitto, le disposizioni delle clausole contrattuali locali di trasferimento prevarranno su quelle delle SCCs "MODULO TRE - Trasferimento da responsabile del trattamento a responsabile del trattamento", nella misura in cui le disposizioni contrastanti delle clausole contrattuali locali di trasferimento solo non pregiudichino i diritti o le libertà fondamentali garantiti agli interessati ai sensi della legislazione europea (in particolare, nella misura in cui i diritti degli interessati siano rispettati).
6.6. Le evidenze del Meccanismo di Trasferimento e l'adempimento dei relativi obblighi costituiscono la documentazione di conformità e formano parte integrante del presente CTDPI.

OBBLIGHI IN TEMA DI COOPERAZIONE E RESPONSABILITÀ

7.1. Il Titolare e il Responsabile si impegnano a collaborare in buona fede per assicurare il rispetto delle previsioni di cui al presente CTDPI, tra cui, ma non solo, il dovere di assicurare il corretto e tempestivo esercizio dei diritti dell'Interessato, gestire incidenti di sicurezza/Violazioni dei Dati Personali al fine di mitigare i possibili effetti avversi da essi derivanti, etc.
7.2 Il Titolare e il Responsabile collaborano in buona fede per rendere disponibile reciprocamente e verso l'Autorità di Controllo le informazioni necessarie a dimostrare il rispetto delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, consentendo e contribuendo il Responsabile alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da un altro soggetto da questi incaricato.

DIRITTI DELL'INTERESSATO

8.1. In considerazione della natura del Trattamento, il Responsabile assiste il Titolare con misure tecniche ed organizzative adeguate ad assicurare l'adempimento degli obblighi del Titolare per riscontrare le richieste per l'esercizio dei diritti dell'Interessato.

8.2. Il Responsabile fornirà al Titolare adeguata cooperazione ed assistenza, e provvederà a fornire tutte le informazioni che possano essere ritenute necessarie per riscontrare l'Interessato o, altrimenti, per permettere al Titolare di dimostrare il rispetto dei propri doveri ed obblighi per quanto concerne i diritti dell'Interessato ai sensi delle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali.

RESTITUZIONE DEI DATI E CANCELLAZIONE

9.1. Il Responsabile, senza porre costi aggiuntivi a carico del Titolare, restituirà o cancellerà i Dati Personali su richiesta del Titolare. Inoltre, alla scadenza o risoluzione anticipata del presente CTDPI il Responsabile, senza porre costi aggiuntivi a carico del Titolare, restituirà o cancellerà i Dati Personali Trattati al Titolare, subordinatamente ad una richiesta da parte del Titolare da comunicare per iscritto con congruo preavviso, salvo che sussistano specifici obblighi di conservazione previsti dalla legge (inclusi, a titolo esemplificativo ma non esaustivo, quelli previsti dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali) o richieste provenienti dall'autorità giudiziaria (tra cui, ma non solo, quelli provenienti dall'Autorità di Controllo), tali da impedire al Responsabile di adempiervi.

9.2. Fatto salvo quanto previsto dall'Art. 9.1, il Responsabile si conformerà alle richieste del Titolare volte alla cancellazione o restituzione dei propri Dati Personali Trattati senza ingiustificato ritardo.

9.3. Nel caso in cui il Titolare richieda la cancellazione dei Dati Personali Trattati e fatto salvo quanto previsto dall'Art. 9.1 e dall'Art. 9.4, il Responsabile fornirà al Titolare un'attestazione che assicuri tale cancellazione senza ingiustificato ritardo.

9.4. Il Responsabile potrà mantenere i Dati Personali trattati che siano conservati con regolari operazioni di backup nel rispetto dei protocolli di *disaster recovery* e *business continuity* del Responsabile, purché il Responsabile non tratti, e non consenta ai propri Sub-Responsabili di trattare, in maniera attiva o intenzionale tali Dati Personali del Titolare per qualsivoglia finalità ulteriore rispetto a quelle stabilite nel presente CTDPI.

VIOLAZIONE DEI DATI PERSONALI

10.1 Il Titolare è consapevole e acconsente che il Responsabile non sarà ritenuto responsabile in caso di Violazione dei Dati Personali che non sia imputabile a negligenza di quest'ultimo.

10.2 Nel caso in cui il Responsabile venga a conoscenza di una Violazione dei Dati Personali, dovrà:

a) adottare le misure appropriate per contenere e mitigare tale Violazione dei Dati Personali, inclusa la notifica al Titolare quanto prima possibile e in ogni caso non oltre quarantotto (48) ore dalla conoscenza della Violazione dei Dati Personali, al fine di consentire al Titolare di implementare rapidamente le contromisure necessarie;
b) collaborare con il Titolare per indagare: la natura, le categorie ed il numero approssimativo di Interessati coinvolti, le categorie ed il numero approssimativo di Dati Personali coinvolti e le probabili conseguenze di tale violazione con modalità commisurate alla serietà ed al suo impatto complessivo sul Titolare ai sensi del presente CTDPI;

c) ove le Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali richiedano la notificazione alle competenti Autorità di Controllo ed agli Interessati della Violazione dei Dati Personali, e nel caso essa si riferisca a Dati Personali del Titolare, il Responsabile dovrà deferire e assumere istruzioni da Titolare, che sarà l'unico ad avere il diritto di determinare le misure che dovranno essere adottate per adempiere alle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali o per porre rimedio a qualsivoglia rischio, tra cui ma non solo:

   i. determinare se l'avviso debba essere fornito a qualsivoglia individuo, autorità di regolamentazione, autorità giudiziaria, enti a tutela dei consumatori o altri come richiesto dalle Disposizioni di Legge Applicabili in materia di Protezione dei Dati Personali, o richiesto a discrezione del Titolare; e

   ii. determinare il contenuto di tale avviso, se sia possibile offrire all'Interessato dalla violazione qualsivoglia tipologia di rimedio riparatorio, nonché la natura e l'estensione di tale rimedio.

MANDATO

11.1 Con la sottoscrizione del presente CTDPI, comprensivo degli Allegati e delle Clausole Contrattuali Tipo, il Titolare dà espressamente mandato al Responsabile a eseguire per conto del Titolare le attività descritte nelle Clausole 5 e 6 di cui sopra.

11.2 Con la sottoscrizione del presente CTDPI, il Responsabile accetta il mandato di cui all'Art. 11.1 di cui sopra, che sarà eseguito senza remunerazione economica, confermando di aver letto e compreso le istruzioni assegnategli.

Per conto di Sapio Produzione Idrogeno Ossigeno S.r.l.:
Nome (scritto per intero):
Posizione:
Firma.....

PTRMRA63L28Z110Q/702800062008600.69.eEtt5QbgP8yudAyT9Wa4+dZ4ZZs=

Firmato digitalmente da PTRMRA63L28Z110Q/7028000620086069.eEtt5QbgP8yudAyT9Wa4+dZ4ZZs=
Data: 2022.11.18 15:42:32 +01'00'

Per conto di Advice Pharma Group S.r.l.:
Nome (scritto per intero):
Posizione:
Firma.....

Firmato digitalmente da:
FERRI ALESSANDRO FLAVIO
Firmato il 10/11/2022 17:23
Seriale Certificato: 16969861
Valido dal 23/01/2020 al 23/01/2023
InfoCert Firma Qualificata 2

ALLEGATO 1 (**Appendice 1 delle Clausole Contrattuali Tipo, ove applicabile)**

A. Elenco delle Parti

Titolare:

Nome: Advice Pharma Group S.r.l.

Indirizzo: Via Arezzo 10/7, 20162 Milano (MI)

Nome, qualifica e dati di contatto del referente

DPO: Avv. Silvia Stefanelli

Dettagli di contatto del DPO: dpo@advicepharma.com

Responsabile:

Nome: Sapio Produzione Idrogeno Ossigeno S.r.l.

Indirizzo: Via San Maurilio n. 13, Milano (MI)

Nome, qualifica e dati di contatto del referente

DPO: Avv. Amleto Zucchi

Dettagli di contatto del DPO: dpo@sapio.it

B. Descrizione del Trattamento/trasferimento: cfr. Allegato 3

Categorie di interessati: cfr. Allegato 3

Categorie di dati personali: cfr. Allegato 3

Frequenza del trattamento/trasferimento: continuativa fino alla cessazione del presente contratto

Natura del trattamento: elettronica, informatica e cartacea

Finalità del trattamento/trasferimento: cfr. Allegato 3

Periodo di conservazione dei Dati Personali oppure, se non è possibile, criteri utilizzati per determinare tale periodo: cfr. Registro delle attività di trattamento

Per i trasferimenti a (sub-)responsabili del trattamento, specificare anche la materia disciplinata, la natura e la durata del trattamento: cfr. Allegato 3

ALLEGATO 2 (**Appendice 2 delle Clausole Contrattuali Tipo, ove applicabile)**

Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile ed i Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

Descrizione delle misure di sicurezza tecniche ed organizzative

Il Responsabile ed i Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte.

L'azienda si affida a un provider (Aruba) certificata ISO 27001.

Informazioni sulle misure di sicurezza

Policy sulla sicurezza informatica

Gestione della sicurezza delle informazioni

La Direzione definisce una serie di politiche e misure per chiarire gli obiettivi al fine di supportare la sicurezza delle informazioni. A livello apicale, è prevista una "Policy per la sicurezza delle informazioni" di carattere generale, come specificato nella sezione 5.2 della ISO/IEC27001.

Organizzazione della sicurezza delle informazioni

Organizzazione interna

L'organizzazione ha definito un Security Officer, sotto la responsabilità del Chief Information Officer. Ove necessario, i compiti sono separati per ruoli e persone al fine di evitare conflitti di interesse e prevenire attività inappropriate.

Dispositivi mobili e telelavoro

È prevista una Policy di sicurezza e adeguati controlli per i dispositivi mobili (come laptop, tablet, PC, dispositivi indossabili, smartphone, strumenti USB e altri) e per il telelavoro (come coloro che lavorano da casa, quelli che viaggiano assiduamente e le postazioni di lavoro da remoto/virtuali).

Sicurezza delle risorse umane

Prima dell'instaurazione del rapporto di lavoro

Le responsabilità della sicurezza delle informazioni vengono prese in considerazione durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e inserite all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).

Durante il rapporto di lavoro

I manager si assicurano che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni. Viene formalizzato un procedimento disciplinare per gestire gli incidenti relativi alla sicurezza delle informazioni presumibilmente causati dai lavoratori.

Conclusione o modifiche al rapporto di lavoro

Vengono gestiti gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la

restituzione delle informazioni e delle apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.

Gestione delle risorse del patrimonio aziendale

Responsabilità delle risorse del patrimonio aziendale

Tutte le informazioni relative alle risorse del patrimonio aziendale vengono inventariate ed i relativi soggetti di riferimento identificati al fine di individuare le responsabilità per la loro sicurezza. Viene definita una Policy per un "uso corretto" delle stesse e le risorse rientrano all'interno dell'organizzazione al momento dell'uscita dei soggetti coinvolti.

Classificazione delle informazioni

Le informazioni sono state classificate e catalogate per direzione, in relazione alle specifiche attività di trattamento individuate per ognuna di esse.

Controllo degli accessi

Requisiti aziendali per il controllo degli accessi

I requisiti previsti dall'organizzazione per controllare l'accesso alle informazioni relative al patrimonio aziendale sono chiaramente documentati in una Policy per il controllo degli accessi e delle relative procedure. L'accesso alla rete e agli applicativi aziendali prevede il superamento di una procedura di autenticazione.

Gestione dell'accesso degli utenti

L'allocazione dei diritti d'accesso da parte degli utenti viene controllata dalla registrazione iniziale dell'utente fino alla rimozione del profilo quando esso non sia più necessario, incluse speciali restrizioni per i diritti di accesso privilegiato e la gestione delle password; peraltro, si procede periodicamente alla revisione e all'aggiornamento dei diritti di accesso.

Responsabilità degli utenti

Gli utenti sono consapevoli delle loro responsabilità attraverso il mantenimento di un effettivo controllo degli accessi, ad es. scegliendo password complesse e mantenendole riservate.

Sistemi e applicazioni per il controllo degli accessi

L'accesso alle informazioni è limitato coerentemente a quanto previsto dalla Policy sul controllo degli accessi, ad es. attraverso autenticazioni sicure, gestione delle password, controllo delle utilità privilegiate e limitazioni all'accesso ai codici sorgente dei programmi.

Crittografia

Controllo crittografico

I dischi dei dispositivi mobili (e.g. laptop, smartphone…) sono criptati mediante soluzioni che rispecchiano lo stato dell'arte. Sono in atto strumenti per la gestione delle chiavi di cifratura. Le schermate di login via web sono protette attraverso TLS.

Sicurezza fisica e ambientale

Aree sicure

La definizione di un perimetro fisico e di una recinzione, con controllo fisico degli accessi e procedure operative, è in grado di proteggere i locali, gli uffici, le stanze, le aree di carico/scarico da accessi non autorizzati. Esistono adeguate procedure e contratti con fornitori esterni per la gestione delle misure contro incendi, allagamenti, terremoti, etc.

Apparecchiatura

L'apparecchiatura (intesa perlopiù come apparecchiatura in ambito ICT), i servizi di supporto e il cablaggio sono resi sicuri e

manutenuti. L'apparecchiatura e le informazioni non possono uscire dal loro luogo di riferimento se non previa autorizzazione, e in ogni caso sono essere adeguatamente protette sia all'interno che all'esterno del loro luogo di riferimento. Le informazioni vengono distrutte prima di procedere allo smaltimento o al riciclo dei dispositivi sui cui erano conservate.

Sicurezza delle operazioni

Procedure e responsabilità operative

Le procedure e le responsabilità operanti per l'area IT sono documentate. I cambiamenti alle infrastrutture ed ai sistemi IT sono controllati. Vengono gestite le singole autorizzazioni. I sistemi di sviluppo, quelli di test e quelli di produzione sono separati.

Protezione da malware

È previsto il controllo dei malware, comprensivo di un'idonea consapevolezza sul punto da parte degli utenti.

Backup

Idonei backup vengono eseguiti e custoditi coerentemente alle policy esistenti, quali Policy sui backup, Disaster Recovery Plan e Business Continuity Plan.

Autenticazione e monitoraggio

La visualizzazione delle attività, le eccezioni, gli errori e gli eventi relativi alla sicurezza delle informazioni da parte degli utenti del sistema e degli amministratori/operatori avvengono previo inserimento delle credenziali di autenticazione. Tali informazioni sono adeguatamente protette. Gli orologi sono sincronizzati.

Controllo di software operativi

L'installazione di software sui sistemi operativi è controllata.

Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche vengono corrette con idonee patch, sono in atto sistemi centralizzati per la gestione degli aggiornamenti e per la loro installazione tempestiva.

Considerazioni sull'audit per le informazioni di sistema

Gli audit per l'area IT sono programmati e controllati per minimizzare l'effetto avverso sui sistemi di produzione o per evitare accesso abusivo ai dati.

Sicurezza delle comunicazioni

Gestione della sicurezza della rete

Le reti e i servizi in rete sono resi sicuri, ad esempio attraverso la loro separazione.

Trasferimento delle informazioni

Sono previste policy, procedure ed accordi (ad es. accordi di riservatezza) relativi al trasferimento delle informazioni verso/da terze parti, compresi i messaggi elettronici.

Acquisizione, sviluppo e manutenzione del sistema

Sicurezza nello sviluppo e processi di supporto

Le modifiche al sistema (sia per le applicazioni che per i sistemi operativi) vengono testate prima di essere inserite in produzione. I pacchetti software non vengono modificati, e vengono osservati i principi di sicurezza ingegneristica. È reso sicuro l'ambiente di sviluppo e controllato lo sviluppo esternalizzato. La sicurezza del sistema viene testata e sono definiti criteri di ammissibilità che includano gli aspetti di sicurezza.

Verifica dei dati di test

I dati utilizzati in ambito di test vengono accuratamente selezionati e controllati.

Rapporti con i fornitori

Sicurezza delle informazioni nei rapporti coi fornitori

Sono previste policy, procedure, sistemi di consapevolezza volti a proteggere le informazioni dell'organizzazione che siano accessibili ai soggetti esterni operanti nell'area IT e ad altri fornitori esterni per l'intera catena di fornitura, concordata nei contratti o negli accordi.

Gestione dei servizi resi dal fornitore

L'erogazione dei servizi resi dal fornitore è monitorata e rivista/verificata in relazione al contratto/accordo. Le modifiche al servizio sono controllate.

Gestione degli incidenti alle informazioni di sicurezza

Gestione degli incidenti sulla sicurezza delle informazioni e miglioramenti

Sono previste responsabilità e procedure (report, valutazioni) volte a gestire in modo coerente ed efficace gli eventi, gli incidenti e le debolezze relative alla sicurezza delle informazioni, anche al fine di conservare prove valide in eventuali giudizi.

Aspetti della sicurezza delle informazioni relativi alla continuità aziendale

Continuità della sicurezza delle informazioni

La continuità della sicurezza delle informazioni è pianificata, implementata e revisionata come parte integrante del sistema organizzativo di continuità aziendale.

Ridondanze

Le strutture IT sono sufficientemente ridondanti per soddisfare i requisiti di disponibilità.

Conformità

Conformità ai requisiti legali e contrattuali

L'organizzazione identifica e documenta i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.

Revisione della sicurezza delle informazioni

I progetti dell'organizzazione relativamente alla sicurezza delle informazioni vengono revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione.

ALLEGATO 3

ATTIVITÀ DI TRATTAMENTO DI DATI PERSONALI

Le seguenti attività di Trattamento possono avere luogo tra le Affiliate del Gruppo Sapio:

A. Information Technology

Descrizione: Trattamento di Dati Personali in relazione alla creazione di account interni sui sistemi e sugli applicativi IT utilizzati all'interno del Gruppo Sapio, audit interni a tali sistemi e applicativi IT, definizione e implementazione delle misure tecniche e organizzative e monitoraggio di tali sistemi e applicativi IT;

Categorie di Interessati coinvolti: dipendenti, altri utenti dei sistemi e applicativi IT del Gruppo Sapio;

Categorie di Dati Personali Trattati: indirizzo IP, indirizzo MAC, User ID, nome, indirizzo e-mail, job title, eventuali altri dati presenti sui sistemi cui accede la Direzione IT in funzione del ruolo svolto dai suoi incaricati di Amministratori di Sistema;

Categorie Particolari di Dati Personali Trattati: N / A.

B. Human Resources

Descrizione: Trattamento di Dati Personali in relazione alla gestione del processo di reclutamento, assunzione di lavoratori, formazione del personale, gestione dei e gestione dei rapporti del fornitore dei benefit per conto del dipendente, gestione delle assenze, gestione della retribuzione dei dipendenti, nonché del pagamento di provvigioni e altre attività necessarie al corretto adempimento del contratto di lavoro;

Categorie di Interessati coinvolti: candidati, dipendenti;

Categorie di Dati Personali Trattati: nome e cognome, dati di contatto (indirizzo e-mail, numero di telefono, indirizzo postale), job title, documento di identità e numero del documento, permessi dal lavoro, informazioni sulle retribuzioni e sulle provvigioni pagate, informazioni contenute nei CV / lettere di presentazione inviate dai candidati;

Categorie Particolari di Dati Personali Trattati: dati relativi all'appartenenza a sindacati, affiliazioni politiche, salute, in quanto necessari alla conformità con gli obblighi applicabili e per esercitare i diritti applicabili nell'ambito del diritto del lavoro, della giustizia e della sicurezza sociale, nonché Categorie Particolari di Dati Personali che i candidati potrebbero scegliere di includere nei propri CV / lettere di presentazione.

C. Legale, Compliance e Gare

Descrizione: Trattamento di Dati Personali in relazione alla gestione di contratti stipulate dalle Affiliate (ad esempio con dipendenti, clienti, fornitori), gestione delle gare d'appalto cui partecipano le Affiliate, gestione delle attività di compliance richieste alle Affiliate e contenziosi relative alle attività delle Affiliate;

Categorie di Interessati coinvolti: dipendenti, clienti, persone di contatto all'interno di clienti (nei casi in cui i clienti sono persone giuridiche), fornitori, persone di contatto all'interno di fornitori (nei casi in cui i fornitori sono persone giuridiche), persone di contatto all'interno della Pubblica Amministrazione, altri soggetti che potrebbero essere coinvolti in pretese avanzate contro / da Affiliate;

Categorie di Dati Personali Trattati: nome e cognome, dati di contatto (indirizzo e-mail, numero di telefono, indirizzo postale), job title, altre categorie di Dati Personali che potrebbero essere rilevanti per la specifica pretesa in questione;

Categorie Particolari di Dati Personali Trattati: le Categorie Particolari di Dati Personali Trattati possono variare a seconda della specifica pretesa in questione (ad esempio dati relative alla salute potrebbero essere compresi in una pretesa relativa allo stato di malattia del dipendente oggetto di controversia); anche Dati Giudiziari potrebbero essere Trattati, ove reati asseriti o effettivamente commessi sono oggetto di controversia.