REGOLAMENTO QUADRO IN MATERIA DI PRIVACY

ORDINE REGIONALE DELLA PROFESSIONE SANITARIA DI FISIOTERAPISTA DELL'UMBRIA (OFI UMBRIA)

I. PREMESSA

Il presente Regolamento quadro in materia di Privacy (il **Regolamento**) è stato redatto su proposta dell'Avv. Alessio Genito, in qualità di DPO dell'Ordine Regionale della Professione Sanitaria di Fisioterapista dell'Umbria - OFI Umbria (di seguito anche solo l'**Ordine**).

Il Regolamento è stato presentato in Consiglio Direttivo dell'Ordine e approvato con Verbale n.1402/2025 del 23.07.2025.

Il Regolamento è uno strumento volto alla corretta gestione dei dati personali da parte dell'ordine, nell'adempimento delle proprie funzioni istituzionali.

Il Regolamento intende inoltre fornire un quadro di soluzioni specifiche a problematiche ricorrenti nella gestione degli adempimenti privacy da parte dell'ordine.

*

II. BASI GIURIDICHE E FINALITÀ DEL TRATTAMENTO DEI DATI PERSONALI

a) *Le funzioni degli ordini professionali*

L'articolo 1, comma 3 del Decreto legislativo del Capo Provvisorio dello Stato 13 settembre 1946, n. 233 - come modificato dalla legge 11 gennaio 2018 numero 3 - dispone, *inter alia* che gli ordini professionali *(i)* promuovono e assicurano l'indipendenza l'autonomia e la responsabilità delle professioni dell'esercizio professionale, *(ii)* verificano il possesso dei titoli abilitanti all'esercizio professionale e curano la tenuta anche informatizzata e la pubblicità anche telematica degli albi dei professionisti *(iii)* partecipano alle procedure relative alla programmazione dei fabbisogni dei professionisti e alle attività formative , nonché all'esame di abilitazione all'esercizio professionale, (*iv*) vigilano sugli iscritti agli albi, in qualsiasi forma giuridica svolgano la loro attività professionale, compresa quella societaria, irrogando le relative sanzioni disciplinari.

Ai sensi dell'articolo 3, comma 1, lett. a) del sopracitato d. lgs. CPS. 233/1946, spetta al Consiglio Direttivo di ciascun Ordine il compito di iscrivere i professionisti nel rispettivo Albo, compilare e tenere gli Albi e pubblicarli all'inizio di ogni anno.

b) ***Il trattamento dei dati personali***

È definita trattamento qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali. La base giuridica è rinvenibile nelle disposizioni normative che rendono lecite determinate attività e/o operazioni di trattamento.

Per tali ragioni, come è stato osservato, il trattamento dei dati personali effettuato dall'ordine professionale, in quanto ente pubblico non economico, viene considerato lecito solo se strettamente necessario ai sensi della normativa di riferimento:

- per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, *lett c,* GDPR);
- per l'esecuzione di un compito connesso all'esercizio di pubblici poteri di cui è investito lo stesso titolare (articolo 6, par. 1, *lett. e.* GDPR).

Alla luce delle precedenti considerazioni, quindi, le finalità di trattamento debbano necessariamente essere connesse ai compiti istituzionali degli ordini professionali che, come visto, riguardano:

- l'organizzazione e la gestione dei procedimenti inerenti all'iscrizione, all'aggiornamento e alla verifica della sussistenza dei requisiti per la permanenza dell'albo professionale;
- l'organizzazione e la gestione degli aspetti finanziari conseguenti all'iscrizione all'Ordine, legati al contributo annuale di iscrizione all'albo;
- la regolamentazione e la gestione della formazione professionale continua, nonché la vigilanza sull' assolvimento di tale obbligo;
- l'invio delle comunicazioni, pubblicazioni o informative a carattere istituzionale a favore degli iscritti.

*

III. MISURE DI SICUREZZA PER LA GESTIONE DEI RISCHI CONNESSI INERENTI AL TRATTAMENTO DEI DATI PERSONALI

Alla luce delle proprie funzioni istituzionali, avuto riguardo del contesto di riferimento e delle dimensioni dell'ente, il Consiglio Direttivo, su proposta del DPO incaricato, predispone adeguate misure di sicurezza in merito al trattamento dei dati dei propri iscritti. Tali misure saranno attuate gradualmente nel corso del triennio 2025 - 2027, su proposta e impulso del DPO incaricato e avvalendosi di collaboratori tecnici e consulenti informatici.

- ***Le misure adottate ed in corso di adozione***

L'Ordine valuta come prioritaria la predisposizione di misure di sicurezza finalizzate alla protezione dei dati personali dai rischi riguardanti eventuali violazioni della riservatezza, della integrità, della disponibilità.

a) Inventario

L'ordine annualmente aggiornerà l'inventario degli hardware, e/o dei dispositivi portatili utilizzati, in via esclusiva o non esclusiva, per l'adempimento delle proprie funzioni istituzionali.

L'inventario dovrà indicare anche i soggetti che possano accedere alla piattaforma *albo web*, nonché la loro qualifica.

b) Definizione dei ruoli

L'Ordine si impegna a confezionare idonea lettera di incarico al personale dipendente e/o autonomo che tratta i dati personali.

I soggetti esterni che trattano i dati per conto dell'Ordine, ivi inclusa la Società che gestisce la piattaforma informatica Albo Web, devono stipulare un accordo ai sensi dell'articolo 28 del GDPR, in qualità di responsabili del trattamento.

c) Policy di sicurezza

L'Ordine ha predispone le policy per l'utilizzo delle attrezzature informatiche, compresa la gestione delle credenziali di autenticazione;

In stretta collaborazione con la Federazione nazionale, l'Ordine predispone un piano di formazione per i soggetti che, a qualunque titolo, trattano per conto dell'Ordine i dati personali degli iscritti.

d) Policy di gestione degli account

L'Ordine si impegna all'utilizzo delle credenziali per accedere ai sistemi informatici a mezzo di password complesse, con relativo rinnovo periodico.

L'Ordine promuove il blocco degli *account* inattivi, e in caso di membri del consiglio direttivo, consulenti, dipendenti, che siano decaduti dalla loro carica o abbiano cessato per qualsiasi ragione la loro collaborazione con l'Ordine.

e) Protezione della posta istituzionale e protezione contro i malware

L'Ordine utilizza *client* di posta elettronica e *browser* pienamente supportati e aggiornati alla versione più recente

L'Ordine protegge adeguatamente tutti i pc (sia postazioni fisse, che portatili) con *software antivirus* regolarmente aggiornati.

f) Gestione dei backup

L'Ordine esegue *backup* periodici, con cadenza mensile, di tutte le risorse in funzione.

L'Ordine archivia i dati su uno spazio di archiviazione regolarmente sottoposto a *backup* accessibile.

g) Protezione dei locali

L'Ordine effettua il controllo dell'accesso ai locali per evitare ingressi non autorizzati., anche attraverso la definizione di una politica di gestione delle chiavi di ingresso e di protezione fisica delle apparecchiature informatiche.

h) Formazione del personale e/o dei soggetti delegati alla privacy all'interno del consiglio direttivo

Di concerto con la Federazione nazionale e con il DPO incaricato, l'Ordine promuove un piano formativo del personale e/o delle risorse incaricate in materia privacy relativamente all' aggiornamento delle disposizioni normative inerenti il trattamento dei dati personali e alla gestione operativa di tali dati

L'Ordine promuove, anche avvalendosi del DPO incaricato la sensibilizzazione del personale e dei membri del consiglio direttivo.

- ***Valutazione di impatto (DPIA)***

La valutazione di impatto si inserisce nel più ampio contesto giuridico sulla protezione dei dati, rappresentato da un approccio basato sul rischio e sulle misure di *accountability*.

Ai sensi della normativa di riferimento in materia di trattamento dati, non tutti i trattamenti effettuati da un titolare devono essere sottoposti a DPIA, ma solo quelli caratterizzati da un rischio elevato.

La struttura organizzativa dell'Ordine ad oggi non impone l'adozione di una valutazione di impatto, la quale sarà adottata entro il triennio di riferimento del presente Regolamento.

Resta inteso che l'ordine ha predisposto le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al trattamento dei dati in relazione alla sua funzione istituzionale.

- ***Le violazioni della sicurezza (data breach)***

Una violazione dei dati personali può compromettere la riservatezza l'integrità o la disponibilità di dati personali.

In caso di violazione, l'articolo 33 del GDPR prevede la notifica al Garante (GPDP), da effettuarsi entro 72 ore dal momento in cui si è venuti a conoscenza della violazione, a meno che si valuti come improbabile un rischio per i diritti e le libertà delle persone fisiche.

Tale notifica di violazione deve essere inviata al GPDP, tramite una apposita procedura telematica, resa disponibile nel portale dei servizi online dell'autorità.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ritardo.

L'Ordine, entro il triennio di validità del presente Regolamento, predisporrà una idonea procedura (la **Procedura**) contenente gli adempimenti in caso di riscontrata violazione della sicurezza. Tale procedura dovrà indicare:

- i soggetti a cui comunicare il *data breach*;
- le azioni da intraprendere per porre rimedio alla violazione;
- la valutazione del *data breach* e le modalità per l'eventuale notifica al garante e per la comunicazione ad interessati;

Nelle more dell'adozione della Procedura, l'Ordine si impegna a comunicare eventuali violazioni al DPO incaricato e a notificarle all'Autorità Garante nei termini di legge. Il processo sarà curato dal consiglio direttivo e dal DPO incaricato.

- ***Il Responsabile per la protezione dei dati***

In quanto enti pubblici non economici a carattere associativo, gli ordini professionali hanno l'obbligo della designazione del DPO ai sensi dell'articolo 37, paragrafo uno, lettera a, del GDPR. La designazione deve essere notificata al garante per la protezione dei dati personali.

Il DPO incaricato deve avere conoscenze specialistiche proporzionate alla sensibilità, complessità e quantità dei dati sottoposti al trattamento.

La capacità di assolvere i compiti da parte del DPO è legata non solo alle qualità professionali e alle conoscenze, ma anche alla sua integrità e ai suoi standard deontologici.

Il DPO incaricato, ai sensi dell'articolo 38 GDPR, è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

È pertanto essenziale che l'Ordine coinvolga il DPO tempestivamente su ogni questione relativa al trattamento e alla protezione dei dati, anche attraverso l'accesso a tutte le informazioni inerenti alle attività che prevedono un trattamento dei dati personali così da fornirgli supporto e input essenziali. Il DPO assicura la propria funzione con indipendenza e autonomia. Il DPO incaricato e responsabile dell'attuazione del presente Regolamento e al suo progressivo aggiornamento; per tale ragione, dovrà relazionare annualmente al consiglio direttivo dell'ordine, partecipando se nel caso alla relativa adunanza.

*

IV. I DATI DEGLI ISCRITTI

Gli iscritti all'albo sottoscrivono idonea informativa relativamente al trattamento dei loro dati personali da parte dell'Ordine.

Come da informativa, che costituisce adempimento propedeutico e obbligatorio ai fini dell'iscrizione all'albo professionale, l'interessato:

- ha diritto di ottenere l'accesso ai dati personali;
- può chiedere che l'ordine, senza giustificato ritardo rettifichi i suoi dati personali inesatti o integri dati incompleti;
- ha diritto di ottenere dall'ordine la cancellazione dei dati personali che loro guardano nei casi espressamente previsti dal GDPR;
- ha diritto di ottenere dall'ordine la limitazione del trattamento quando ricorre uno dei casi espressamente previsti dal GDPR;
- ha diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano connessi a ragioni di interesse pubblico o all'esercizio di pubblici poteri.

*

V. INDIVIDUAZIONE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI

Con riferimento ai soggetti autorizzati a trattare dati all'interno dell'Ordine, dovranno essere designati, con apposito atto di nomina, eventuali dipendenti, collaboratori anche a titolo di consulenziale e le figure apicali.

*

VI. AGGIORNAMENTO E IMPLEMENTAZIONE DEL PRESENTE REGOLAMENTO

L'aggiornamento e l'implementazione del presente Regolamento sarà predisposta annualmente dal DPO incaricato, il quale proporrà le proposte di modifica e/o integrazione al Consiglio Direttivo per la definitiva approvazione.

Gli adempimenti scaturenti dal presente Regolamento saranno curati dal Consiglio Direttivo dell'Ordine, nonché dal DPO incaricato.

*

VII. PUBBLICAZIONE E VALIDITA'

Il presente Regolamento viene pubblicato, non oltre un mese dalla sua adozione, sul sito istituzionale dell'Ordine, Sezione *amministrazione trasparente*.

Il presente Regolamento ha efficacia triennale.

Perugia, 31.08.2025

Presidente dell'Ordine Ordine Regionale della Professione Sanitaria di Fisioterapista dell'Umbria (OFI Umbria)
Dott.ssa Daniela Gaburri

[redacted]

Il DPO incaricato
Avv. Alessio Genito

[redacted]

Firme autografe omesse ai sensi dell'art. 3 del D.Lgs. n.39/1993