REGOLAMENTO PRIVACY E PROTEZIONE DEI DATI PERSONALI

1. **Premesse**

   La Tesip – Tecnologie e Sistemi Informativi Previdenziali srl (di seguito, per brevità "Tesip") adotta il presente Regolamento - suscettibile di costante aggiornamento – al fine di conformarsi alle disposizioni in materia di Privacy e protezione dei dati personali previste dal General Data Protection Regulation, ovvero Regolamento UE 679/2016 (di seguito, per brevità "GDPR" o "Regolamento UE"), applicabile a partire dal 25 maggio 2018.

   La Tesip garantisce che i trattamenti dei dati personali si svolgano nel rispetto dei diritti e delle libertà fondamentali dell'interessato e della normativa in materia, sensibilizzando in tal senso tutti i membri del personale.

2. **La nuova normativa privacy alla luce del Regolamento UE 679/2016**

   Il GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi, è volto ad armonizzare tutte le normative in materia di Privacy presenti all'interno dell'Unione Europea.

   Il Regolamento UE muta l'approccio al tema della protezione dei dati personali, rafforzando ed incrementando la tutela dei diritti dell'interessato ed affidando un ruolo pro-attivo al Titolare ed al Responsabile del trattamento, accrescendone così la cd. accountability.

   Inoltre, il Regolamento UE mira a focalizzare l'attenzione di tutte le figure coinvolte sul rispetto e sulla conformità dei trattamenti effettuati alla normativa europea.

   Quanto all'ambito di applicazione, il GDPR supera il principio della territorialità e si applica a tutti i trattamenti di dati personali da parte di Titolari non necessariamente stabiliti nell'Unione Europea, purché questi riguardino beni, servizi o comportamenti degli interessati all'interno dell'UE.

3. **Principi del Trattamento**

   La Tesip effettua il trattamento dei dati personali relativi agli iscritti, comunicati dai Collegi provinciali in occasione dell'iscrizione all'Albo o conferiti direttamente dai professionisti all'avvio o nel corso del rapporto con l'Ente, ovvero altrimenti acquisiti nell'ambito della normale attività istituzionale dell'Ente, nel rispetto delle norme vigenti e nelle forme e nei limiti previsti dalla legge.

   Il trattamento ha ad oggetto i dati, anche di natura sensibile, necessari all'espletamento dell'attività istituzionale dell'Ente, per scopi previdenziali e

assistenziali e/o per fini connessi e strumentali all'esercizio della professione di perito industriale e per ogni altra finalità derivante da obblighi di legge, da regolamenti e dallo statuto, nonché da disposizioni di Autorità legittimate dalla legge e da organi di vigilanza e di controllo.
Il trattamento dei dati personali da parte della Tesip è effettuato nel rispetto dei principi
di cui all'art. 5 GDPR e, nello specifico:

a. liceità, correttezza e trasparenza nei confronti dell'interessato;
b. limitazione della finalità del trattamento;
c. minimizzazione della raccolta dei dati;
d. esattezza dei dati rispetto alle finalità per le quali vengono trattati;
e. limitazione temporale della conservazione dei dati;
f. integrità e riservatezza;
g. responsabilizzazione del titolare.

4. Definizioni

Ai fini di una agevole comprensione del Regolamento, si riportano alcune delle definizioni contenute nell'art. 4 del Regolamento UE:
"dato personale": 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;
"trattamento": 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;
"*titolare del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati personali;
"*responsabile del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare;
"*destinatario*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
"*autorità di controllo*": l'autorità pubblica indipendente istituita da uno stato membro ai sensi dell'art. 51 GDPR
"*profilazione*": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti

riguardanti il rendimento professionale, la situazione economica, la saluta, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
"*consenso dell'interessato*": qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
"*violazione dei dati personali*": la violazione di sicurezza che comporta accidentalmente in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata l'accesso ai dati personali trasmessi, conservati o comunque trattati.

5. Tipologia trattamenti

Sono individuate le seguenti tipologie di trattamento:

- gestione anagrafica iscritti EPPI/Albo; gestione degli obblighi contributivi; erogazione delle prestazioni previdenziali e assistenziali il tutto come previsto dalla normativa di riferimento e dallo Statuto dell'Ente socio;
- esecuzione di obblighi derivanti da contratti, accordi e convenzioni;
- adempimento di obblighi di legge di natura amministrativa, contabile, civilistica, fiscale, regolamenti, normative comunitarie ed extracomunitarie;
- gestione della clientela (acquisizione dati e informazioni precontrattuali, amministrazione della clientela, amministrazione dei contratti, ordini, spedizioni e fatture);
- gestione del contenzioso (inadempimenti contrattuali; diffide, transazioni, recupero crediti, arbitrati, controversie giudiziarie);
- gestione del personale dipendente;
- gestione e controllo accessi presso ns. sede;
- compimento di ricerche di mercato;

6. Finalità del trattamento

Con il presente Regolamento la Tesip garantisce che i trattamenti di cui al paragrafo che precede vengano effettuati per finalità strettamente connesse all'attività svolta dalla Tesip, prevalentemente per la gestione dei sistemi informativi ad essa delegata in qualità di società in house providing, dal socio unico EPPI. Il rapporto tra l'ente socio e la società è disciplinato da un'apposita convenzione di servizi funzionale alla gestione dei dati degli iscritti all'EPPI.
Inoltre in relazione alla normativa di settore ed allo statuto dell'ente socio, la società in forza di apposito accordo tra l'ente socio ed il CNPI, gestisce i dati personali presenti nell'Albo Unico dei periti industriali.

7. Banche dati

Per banca dati si intende il complesso organizzato di una o più unità, dislocate in uno o più siti. La Tesip, in particolare, utilizza banche dati di tipo cartaceo ed informatico, software gestionali.

8. I soggetti del trattamento

La Tesip individua quali soggetti coinvolti nel trattamento dei dati personali le figure di seguito riportate.

7.1 Titolare

Il Titolare del trattamento è la Tesip - in persona del Presidente - in quanto esercita un potere decisionale autonomo in merito alle finalità ed i mezzi del trattamento dei dati personali degli iscritti.

Ai sensi dell'art. 24 del GDPR il Titolare mette in atto le misure tecnico-organizzative adeguate per garantire la conformità del trattamento ai principi di cui al Regolamento.

7.2 Responsabile del trattamento

Attesa la molteplicità delle funzioni, la Tesip è articolata attraverso dei Responsabili interni del trattamento individuati nei Responsabili di funzione e dei Responsabili esterni.

Sono Responsabili esterni tutti i soggetti esterni alla Tesip che effettuano trattamenti sulle banche dati dello stesso, per suo conto e nel suo interesse; qualora, invece, questi determini autonomamente le finalità ed i mezzi del trattamento, deve considerarsi titolare dei trattamenti in questione.

I trattamenti da parte del Responsabile (interno o esterno) del trattamento sono disciplinati, ai sensi dell'art. 28 GDPR, da un contratto o altro atto giuridico che individui la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate al Responsabile, gli obblighi ed i diritti del Titolare.

Il Responsabile del trattamento non può trattare i dati personali se non secondo le istruzioni impartite dal Titolare ed in caso di trattamenti particolarmente complessi può nominare, a sua volta, un sub-responsabile.

7.3 Persone autorizzate al trattamento (ex "incaricati")

Ai sensi dell'art. 29 GDPR, il Titolare o il Responsabile del trattamento individua - con apposite nomine e quali persone autorizzate al trattamento medesimo – i soggetti (es, dipendenti) che intervengono, in relazione all'esercizio delle rispettive mansioni e competenze, nell'esecuzione dei trattamenti.

Le persone autorizzate al trattamento dei dati personali agiscono, dunque, sotto l'autorità del Responsabile o del Titolare del trattamento.

7.4 Responsabile della Protezione dei Dati (Data Protection Officer, "DPO")

Ai sensi del GDPR, il Titolare designa un Responsabile della Protezione dei dati con comprovate conoscenze in materia di privacy.

Il Responsabile della Protezione dei dati può essere un dipendente della Tesip o un soggetto esterno nominato in virtù di un contratto di servizi.

Ai sensi dell'art. 39 GDPR, il DPO ha, tra gli altri, il compito di:

- informare e fornire consulenza al Titolare o al Responsabile del trattamento;
- sorvegliare l'osservanza della normativa in materia di protezione dei dati personali,
compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale
della Tesip che partecipa ai trattamenti;
- fornire pareri, se richiesti;
- cooperare con l'autorità di controllo.

7.5 amministratore di Sistema

Il Codice non prevede una definizione tipica di Amministratore di sistema, tuttavia questo può definirsi "*il soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione*". Le funzioni tipiche dell'amministrazione di un sistema vanno dalla realizzazione di copie di sicurezza (operazioni di *backup* e *recovery* dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

9. Diritti dell'interessato

Il Regolamento riconosce l'esercizio da parte dell'interessato dei diritti di cui agli artt. 15-21 del GDPR e, nello specifico: il diritto di accesso ai dati, di rettifica ed il diritto alla cancellazione ("diritto all'oblio") degli stessi, il diritto di limitarne il trattamento, il diritto alla loro portabilità, nonché il diritto di opposizione al trattamento.

10. Sicurezza del trattamento

Il Titolare ed il Responsabile del trattamento garantiscono, ai sensi dell'art. 32 GDPR, un livello di sicurezza adeguato al rischio per i diritti e le libertà degli interessati, adottando misure tecnico-organizzative, fra le quali:

- la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità,
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali
- ed, in generale, la manutenzione dei sistemi informatici;
- una procedura per testare regolarmente l'efficacia delle misure adottate per prevenire e/o fronteggiare i potenziali rischi del trattamento.

11. Consenso dell'interessato

Ogni qualvolta il trattamento dei dati personali richieda il consenso dell'interessato, tale consenso dovrà essere conservato e registrato.
L'interessato deve poter conoscere le modalità per prestare il consenso ed ha diritto - ogni qualvolta lo stesso venga richiesto ai fini del trattamento – di revocarlo in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore di età inferiore ai 16 anni, il Responsabile della Protezione dei Dati deve garantire che il consenso dell'esercente la responsabilità genitoriale sia fornito prima della raccolta.

12. Informativa privacy

Ai sensi degli artt. 13 e 14 GDPR, la Tesip fornisce all'interessato informazioni specifiche, chiare e sintetiche - sia nel caso di dati raccolti presso l'interessato che di dati raccolti presso terzi - sui trattamenti che intende effettuare.

13. Notifica di una violazione dei dati personali all'autorità di controllo

Il Titolare del trattamento è tenuto a notificare, secondo le modalità di cui all'art. 33 n. 3 GDPR, l'eventuale violazione dei dati personali – di cui sia venuto a conoscenza direttamente o su informazione del Responsabile del trattamento - all'autorità di controllo competente *ex* art. 55 del Regolamento UE, salvo che il rischio venga valutato come improbabile per i diritti e le libertà dell'interessato.

Ad ogni modo il Titolare, nel rispetto del principio di *accountability*, documenta qualsiasi violazione, così da consentire all'autorità di controllo di verificare la conformità del trattamento alla normativa vigente.

14. Comunicazione di una violazione all'interessato e trasparenza

Il Titolare del trattamento, altresì, comunica la violazione di dati personali all'interessato, qualora questa presenti rischi elevati per i diritti e le libertà dello stesso e salvo che non ricorrano le condizioni di cui all'art. 34 n. 3 GDPR.

15. Sanzioni

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è punito con l'applicazione di sanzioni amministrative pecuniarie, inflitte secondo i criteri di cui all'art. 83 GDPR ed, in generale, tenuto conto della natura della gravità e della durata della violazione, delle finalità del trattamento, del numero degli interessati lesi, del livello del danno e dell'aspetto doloso o colposo della violazione.

Resta ferma l'applicabilità di sanzioni penali, conformemente a quanto previsto dalla legislazione nazionale in materia.

16. Disposizioni finali

Per quanto non espressamente previsto nelle presenti Linee Guida, si applicano le disposizioni del Regolamento (UE) 2016/679 e dei provvedimenti del Garante per la protezione dei dati personali.

Roma, giugno 2018

Ruolo	Funzione	Incaricato
Responsabile protezione Dati (Data protection Officer – DPO)	Ai sensi dell'art. 39 GDPR, il DPO ha, tra gli altri, il compito di: - informare e fornire consulenza al Titolare o al Responsabile del trattamento; - sorvegliare l'osservanza della normativa in materia di protezione dei dati personali, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale della Tesip che partecipa ai trattamenti; - fornire pareri, se richiesti; - cooperare con l'autorità di controllo	INTERNO
Responsabile del trattamento	Attesa la molteplicità delle funzioni, la Tesip è articolata attraverso un Responsabile interno del trattamento individuato nel Direttore Tecnico e dei Responsabili esterni. Sono Responsabili esterni tutti i soggetti esterni alla Tesip che effettuano trattamenti sulle banche dati dello stesso, per suo conto e nel suo interesse; qualora, invece, questi determini autonomamente le finalità ed i mezzi del trattamento, deve considerarsi titolare dei trattamenti in questione. I trattamenti da parte del Responsabile (interno o esterno), sono disciplinati, ai sensi dell'art. 28 GDPR Il Responsabile del trattamento non può trattare i dati personali se non secondo le istruzioni impartite dal Titolare ed in caso di trattamenti particolarmente complessi può nominare, a sua volta, un sub-responsabile.	INTERNI - Direttore tecnico ESTERNI - CDA - Collegio sindacale - Fornitori - Consulenti
Amministratore di sistema	L'Amministratore di sistema è il soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione". Le funzioni tipiche dell'amministrazione di un sistema vanno dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione. In considerazione del modello organizzativo della Tesip, sono stati individuate le seguenti figure: A. network administrator; B. Data Base administrator;	INTERNI Responsabile interno incaricato

Ruolo	Funzione	Incaricato
	C. Gestore dei back-up e restore.	