# Linee Guida sulla sicurezza del trattamento dei dati personali

## Consiglio Nazionale dei Periti Industriali e dei Periti Industriali Laureati

| | | | |
|---|---|---|---|
| ***Codice documento*** | P_001 | ***Versione:*** ***del*** | 10/07/2025 |
| ***Preparato da:*** | Alavie Srl | ***Verificato da:*** ***Approvato da:*** | *Marcella Di Guida* CNPI |

# INDICE

## Scopo del documento

Le presenti Linee Guida per la sicurezza informatica sono state redatte tenendo conto delle linee guida del Regolamento UE 2016/679.

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete internet dei PC, espone il Consiglio Nazionale dei Periti Industriali e Periti Industriali Laureati (più avanti definita anche CNPI o Ente o titolare o datore di lavoro) e gli utenti (dipendenti, collaboratori e consiglieri della stessa) giuridica, reputazionale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, creando evidenti problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, CNPI ha adottato il presente regolamento, per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano arrecare problemi o minacce alla Sicurezza nel trattamento dei dati.

Le Linee Guida di seguito riportate vanno incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e dei consiglieri e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza e la riservatezza informatica di tutta l'azienda.

È necessario, quindi, osservare scrupolosamente le seguenti regole allo scopo di impedire, per quanto possibile, attacchi informatici di vario tipo.

I trasgressori della presente disposizione saranno ritenuti responsabili dei danni direttamente o indirettamente causati oltre che sanzionati secondo gli articoli disciplinari del CCNL.

Si ricorda che in caso di eventuali problematiche è bene avvisare il proprio Responsabile IT.

## Utilizzo della strumentazione hardware

1.1. Il Personal Computer (PC) affidato al dipendente è uno strumento di lavoro.

Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.

Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire a generare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il PC deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

1.2. Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati.

Non è consentita l'installazione di programmi diversi da quelli autorizzati dalla direzione.

Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della legge n. 128 del 21.05.2004.

1.3. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il diretto responsabile nel caso in cui siano rilevati virus e adottando quanto previsto nei successivi punti.

1.4. È fatto divieto d'installare componenti hardware fissi o removibili sulla strumentazione in uso se questo non risulta espressamente richiesto ed autorizzato dall'Ente.

L’Ente si riserva di eliminare qualsiasi componente hardware la cui installazione non sia prevista o sia stata appositamente autorizzata.

1.5. Qualora si rendessero necessarie modifiche sostanziali alle configurazioni di base impostate sul PC in uso, occorre darne comunicazione al Titolare del Trattamento e all’IT.

Il PC deve essere spento ogni sera prima di lasciare gli uffici (salvo diverse disposizioni della Direzione e per esigenze lavorative previamente comunicate dall'Ente) o in caso di assenze prolungate dall’ufficio o di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l’indebito uso, pertanto è necessario attivare il blocco dello schermo quando ci si allontana dalla postazione.

1.6. più in generale ogniqualvolta ci si allontana dalla postazione di lavoro il PC deve essere bloccato effettuando le seguenti operazioni:

- digitare "CTRL+ALT+CANC"
- scegliere "Blocca computer"
- oppure
- usare il tasto appositamente previsto per i PC che ne sono dotati
- eventualmente è possibile prevedere un blocco automatico tramite screen saver.

L'Utente deve inoltre applicare gli accorgimenti disponibili per rendere il PC protetto da accessi abusivi, come ad esempio, quando possibile, chiudere a chiave la porta, depositare il PC in un armadietto con chiave, ecc.

1.7. Gli assegnatari di PC portatili devono conservare e proteggere i PC a loro consegnati in modo tale da ridurre al minimo eventuali rischi di perdita, danneggiamento e/o furto del PC stesso.

## Accesso ed uso dei sistemi informatici aziendali (credenziali di autenticazione)

2.1. Sulla base della vigente normativa privacy, i requisiti minimi di complessità delle password sono:

- redazione con caratteri maiuscoli e/o minuscoli;
- composizione con inclusione di simboli, numeri, punteggiatura e lettere;
- numero di caratteri non inferiore ad 8 (ad eccezione dei sistemi che non supportano tali requisiti);
- password non agevolmente riconducibile all'identità del soggetto che la gestisce.

Pertanto, la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa. A mero titolo esemplificativo e non esaustivo, la password non deve essere: il nome o il cognome dell'Utente, il soprannome, la data di nascita propria, dei figli o degli amici, non deve consistere in un nome di un hobby o di una passione conosciuta o facilmente conoscibile da colleghi o conoscenti, non deve riprodurre il nome e/o cognome di personaggi famosi.

2.2. Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a sostituirla.

2.3. Non devono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o "remember password", presenti nei browser o in altre applicazioni che gestiscono la procedura di autenticazione.

2.4. L'Utente ha l'obbligo di non alterare la funzione "cambio password" in riferimento alla previsione di modificare la password con cadenza trimestrale.

2.5. Tutti gli Utenti hanno la possibilità di modificare la propria password in qualsiasi momento, purché ciò avvenga non oltre un arco temporale di 90 giorni.

E' obbligatorio procedere alla modifica tempestiva della password quando:

- le credenziali, per ragioni di servizio, siano state trasmesse ad un collega in caso di personale assenza;
- incaricati o addetti non autorizzati ne siano venuti a conoscenza.

Nel caso di utilizzo di riconoscimento biometrico o facciale, il cambio password periodico può essere evitato.

## Installazione di programmi sui PC o Server dell'Ente

3.1. Sul PC o Server in uso non devono essere installati programmi che non siano ufficialmente autorizzati dal Titolare del Trattamento.

3.2. È vietato il download e l'utilizzo di programmi, ancorché gratuiti, se non per esigenze comprovate e previa esplicita autorizzazione del Titolare del Trattamento.

3.3. L'Ente, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi del D.Lgs 231/01.

3.4. Eventuali illeciti che dovessero essere commessi utilizzando la strumentazione informatica aziendale potranno essere oggetto di sanzioni disciplinari.

## Utilizzo di altri dispositivi elettronici

4.1. Tutti i dispositivi elettronici dati in dotazione al personale e/o ai consiglieri, devono considerarsi strumenti di lavoro e ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative.

4.2. Fra i dispositivi in questione vanno annoverati i telefoni aziendali, i tablet, i telefoni cellulari, gli smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete dell'organizzazione o di condividere documenti, dati e materiali ivi conservati e/o trattati.

4.3. Nel caso in cui l'Utente sia stato dotato dall'Ente di un dispositivo smartphone o tablet, lo stesso dovrà essere custodito e utilizzato con diligenza, in particolare nel caso in cui l'Utente decida di installare ulteriori App rispetto a quelle già installate. Va sottolineato, infatti, che un'app è un software che permette di interconnettersi con le informazioni (dati personali) e gli strumenti su cui è installata. L'utente dovrà porre particolare attenzione alle richieste di accesso alle immagini, ai contatti in rubrica, l'accesso al microfono e alla fotocamera, l'accesso ai file in memoria, l'accesso ai dati sulla geolocalizzazione, la gestione dei cookie. Si raccomanda di utilizzare consapevolmente i dispositivi assegnati, per preservare la riservatezza dei dati aziendali ma anche per

tutelare i propri dati personali, ed evitare comportamenti illeciti come la condivisione di contatti, foto, video e documenti di vario genere senza il consenso di tutte le persone coinvolte.

## Utilizzo di supporti magnetici e dati

5.1. Tutti i supporti magnetici rimovibili, contenenti dati sensibili nonché informazioni costituenti know-how interno, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto.

5.2. Ove possibile, è necessario conservarli in locali o armadi sicuri, è proibito usarli a scopi personali.

5.3. In caso di rilevamento virus è necessario avvisare l'IT tempestivamente.

5.4. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

5.5. Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere segnalati, ed eventualmente sottoposti al controllo e relativa autorizzazione all'utilizzo da parte del Titolare del Trattamento.

## Utilizzo della rete interna

6.1. La rete interna, che consente la connessione a Internet ed il collegamento tra gli utenti all'interno della stessa sede, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.

6.2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni istituzionali, deve essere impegno di ciascun Utente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

6.3. L'utilizzo di DFS (Domaine File System) per la condivisione di dati è concesso soltanto agli Utenti di CNPI. Deve essere interesse di ciascun Utente preservare dati, notizie ed informazioni istituzionali dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati. La condivisione di dati appartenenti a CNPI con soggetti esterni, è ammessa per esigenze progettuali, solo tramite mail istituzionali. Nel caso di dubbi, consultare il Titolare del Trattamento

## Utilizzo della rete esterna internet

7.1. Il PC assegnato al singolo utente e abilitato alla navigazione in Internet e costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

7.2. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware o a pagamento, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;

- l’effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi casi direttamente autorizzati dalla Direzione;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all’attività lavorativa;
- la partecipazione a Forum non professionali, l’utilizzo di chat online (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books, anche utilizzando pseudonimi (o nicknames), se non espressamente autorizzati dal responsabile di riferimento;
- navigare in siti non attinenti allo svolgimento delle mansioni assegnate (per es. siti web di giochi online di ogni tipo e natura (casualità, giochi di abilità, ecc.)); siti dove è possibile visualizzare e/o ascoltare in streaming audio e/o video; siti per adulti, ecc.);
- non è consentito l’utilizzo di sistemi di scambio di documenti e/o di archiviazione di massa a distanza (per es. ma non solo, Dropbox, ecc.), salvo espressa autorizzazione del Titolare del Trattamento e privilegiando le risorse aziendali in essere (DFS)

7.3. Non possono essere utilizzati modem privati, o reti di terzi senza autenticazione, per il collegamento alla rete, e l'utilizzo della rete Internet deve essere limitato al tempo strettamente necessario alle operazioni professionali da svolgere.

Non utilizzare reti internet (ad esempio reti Wi-Fi in luoghi pubblici) sconosciute.

7.4. Eventuali controlli specifici (per es. log di connessioni effettuate da una singola postazione, con particolare riferimento a navigazione su siti illeciti o non attinenti all’attività lavorativa), saranno preventivamente notificati e conservati nel rispetto dei limiti previsti dalla normativa vigente.

## Utilizzo della posta elettronica

8.1. La casella di posta elettronica assegnata all’Utente (da intendersi come ogni soggetto che utilizza utenza e/o device collegati a CNPI) è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.).

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all’attività lavorativa. In questo senso, a titolo puramente esemplificativo, l’utente non potrà utilizzare la posta elettronica per:

- l’invio e/o il ricevimento di allegati contenenti filmati non legati all’attività lavorativa;
- l’invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, convegni, concorsi, forum o mailing list se non per finalità strettamente lavorative;
- inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita.

8.2. È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti).

8.3. Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

Nel caso di messaggi provenienti da mittenti conosciuti, ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

Non diffondere/inoltrare la mail a colleghi e/o al Titolare del Trattamento (Datore di Lavoro); segnalare la mail sospetta all'IT.

8.4. Le caselle di posta elettronica assegnate all'Utente sono destinate ad un utilizzo di tipo aziendale. L'invio e la ricezione di e-mail personali devono essere considerati come una pratica residuale.

8.5. La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".

Nel caso in cui si debba inviare un documento all'esterno dell'azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg).

Per quanto riguarda i messaggi di posta elettronica in entrata, laddove l'utenza Office 365 attribuita all'Utente lo consenta, la memorizzazione dovrà avvenire sul PC in locale, con conservazione massima di 24 mesi decorrenti dalla ricezione.

8.6. La casella di posta deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.

8.7. L'account di posta elettronica aziendale sarà disattivato al termine del rapporto di lavoro e dovrà essere prevista una mail di risposta automatica, in cui verrà indicata la disattivazione della stessa e la nuova mail a cui fare riferimento. Decorsi i 30 giorni dalla disattivazione della casella di posta, l'account sarà chiuso e cancellato al termine dei 6 mesi successivi. L'accesso a questa casella di posta, in questo periodo di tempo tra la cessazione del rapporto di lavoro con l'Utente e la cancellazione, potrà avvenire solo tramite log dell'Amministratore di Sistema e/o della sola persona preposta e nominata alla gestione di questa attività.

Inoltre, in merito alla raccolta dei metadati nei sistemi di posta, come da Provvedimenti del Garante, è previsto un termine di conservazione non superiore ai 21 giorni.

## Backup e crittografia

9.1. Ogni Utente ha la responsabilità di effettuare il backup periodico dei dati contenuti nel proprio PC. A tal fine, ogni utente dovrà utilizzare come repository dei dati lo spazio disponibile nell'ambito del proprio "DFS".

9.2. L'utilizzo dello spazio disponibile su DFS garantisce un continuo backup e la possibilità di poter accedere ai propri dati anche da postazioni remote.

9.3. I dati contenuti nel proprio PC, quandanche replicati tramite meccanismo di sincronizzazione con DFS, devono essere obbligatoriamente crittografati tramite l'utilizzo delle funzionalità disponibili nei PC. La modalità di attivazione della funzionalità deve essere richiesta al gestore dei sistemi informatici.

## Utilizzo Dei Social Media

10.1. L'utilizzo dei social media, quali Facebook™, Linkedin™, dei blog e dei forum, è consentito durante l'orario di lavoro soltanto per finalità professionali e attinenti l'attività lavorativa.

10.2. Un loro, eventuale, utilizzo a fini promozionali e commerciali viene gestito e definito dall'organizzazione secondo le seguenti regole comportamentali, che consentono di tutelare l'immagine e il patrimonio dell'Ente da una parte e i collaboratori, i propri clienti, fornitori e partners dall'altra:

- la condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni istituzionali considerate dall'Ente riservate ed in genere sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partner dell'organizzazione stessa;
- ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'organizzazione;
- l'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo ed espresso personale consenso di questi, e comunque non potrà postare sui social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo ed espresso consenso del Responsabile d'area;
- l'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere nei confronti di terzi, dell'organizzazione, dei colleghi, dei clienti e dei fornitori, attività che possano essere penalmente o civilmente rilevanti (ad es. sono vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie).

La policy qui dettata deve venir seguita dagli utenti anche nel caso in cui utilizzino propri dispositivi e partecipino ai social media a titolo personale.

## Minacce e attacchi virali

11.1. Il sistema informatico-telematico dell'Ente è protetto da attacchi di virus informatici e da attacchi dall'esterno attraverso apparecchiature Firewall e Antivirus; questa infrastruttura è necessaria per garantire l'incolumità e protezione dei dati in esso contenuti, nel rispetto del patrimonio aziendale e della legge sulla Privacy. Inoltre, ogni singolo PC prevede all'interno il sistema operativo più recente e contestualmente si sono adottati software di protezione diretta sulle workstation, server e altri device.

11.2 Al fine di garantire lo standard di protezione adottato non è possibile effettuare operazioni che possano mettere in pericolo l'incolumità del sistema, salvo autorizzazione del Titolare del Trattamento. In particolare, è necessario seguire le seguenti regole:

- non scaricare file dalla rete internet se non si è ragionevolmente certi dell'attendibilità della fonte (per es. portali su cui si è autenticati). L'attendibilità può essere verificata attraverso l'utilizzo di servizi disponibili sul Web (per es. www.virustotal.com) e nel caso di dubbi contattare l'IT;
- non comunicare attraverso chat-line o altri sistemi simili se non con sistemi garantiti e certificati (per es. Microsoft Teams);
- non accedere a siti che richiedono l'installazione di certificati;
- non iscriversi a siti internet, newsletter, bacheche elettroniche, guest book, community e ad altra attività similare che richiede il rilascio di identificazione personale o aziendale, se non strettamente attinenti alle attività lavorative;
- non introdurre qualsiasi supporto digitale di tipo personale, se non di provenienza certa e verificata, quali ad esempio: CD-Rom, chiavette USB, HD esterni, cellulare, macchine fotografiche digitali.

11.3 Il software di protezione installato su tutti i PC segnala immediatamente l'eventuale rilevamento di Virus. In questo caso, l'Utente è tenuto a rimuovere immediatamente il Virus (sempre mediante il programma Anti-Virus); è tenuto inoltre ad avvisare l'IT, affinché sia avviata una ricerca per scoprirne la provenienza ed evitare il ripetersi dell'incidente.

11.4 Ogni Utente di PC deve disinstallare qualsiasi software che sia stato installato non ottemperando alle indicazioni fornite in precedenza.

## Webcam

12.1 Le Webcam e gli altri sistemi di audio-videoripresa possono ricadere sotto il provvedimento del Garante della videosorveglianza del 8 aprile 2010, che prevede una serie di accorgimenti e restrizioni all'uso degli stessi12.3. Di conseguenza si richiede ad ogni Utente dotato di tali sistemi di:

- utilizzare le webcam solo per necessità collegate strettamente alle attività lavorative;
- non lasciare collegato il sistema di audio-videoripresa se non necessario;
- ricordarsi di scollegare il sistema di audio-videoripresa al termine dell'utilizzo dello stesso.

## Applicazione ed interpretazione del presente regolamento

13.1. Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, l'Utente può rivolgersi al Titolare del Trattamento.

13.2. Qualora l'Utente violi anche una sola delle presenti prescrizioni, potranno essere emanati provvedimenti disciplinari come da CCNL applicato.

133. Resta inteso che qualora la violazione dovesse concretizzarsi nella commissione di un reato rilevante, l'Ente si riserva di procedere per la salvaguardia della propria posizione e di terzi parti offese (in tal senso si fa particolare riferimento al download di opere protette – musica o film – nonché di navigazioni su siti illeciti).

13.4. I precetti normativi, ai sensi del Regolamento UE 2016/679, in caso di data breach che determina un pericolo per i diritti e le libertà degli interessati, impongono al Titolare del

trattamento la notifica al Garante per la Protezione dei Dati Personali il termine perentorio di 72 ore dal momento in cui ne è venuto a conoscenza, salvo casi particolari. Pertanto, il comportamento dell'utente, in caso di data breach, è l'immediata segnalazione all'IT ed al Datore di Lavoro in qualità di Titolare del trattamento, che deve procedere alla notifica.

## Disciplina deroghe e modifiche delle presenti Linee Guida

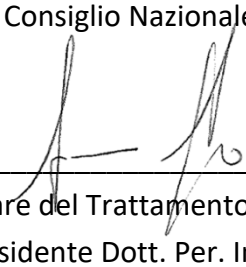
14.1. Sono parte integrante delle presenti Linee Guida le circolari istituzionali.

Le circolari (o comunicazioni interne) sono documenti che hanno lo scopo di rendere pubbliche ai dipendenti le disposizioni dell'Ente, normative, operative e comportamentali che si rendano necessarie a seguito dell'evolversi dell'attività o di nuovi adempimenti.

Nel caso in cui si rendessero necessarie eventuali modifiche o integrazioni alle presenti Linee Guida, che prevedano di fatto un' implementazione delle misure adottate, le stesse saranno prontamente notificate dall'organizzazione all'Utente.

Il presente regolamento è entrato in vigore a far data dal 10 settembre 2025.

Per il Consiglio Nazionale dei Periti Industriali e dei Periti Industriali Laureati



_____

Titolare del Trattamento dei Dati

Il Presidente Dott. Per. Ind. Giovanni Esposito