Ordine delle Professioni Infermieristiche di Torino

ANAGRAFICA

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

SEDE LEGALE	Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

NUOVE REGOLE IN MATERIA DI PRIVACY

PREMESSA

Dal 25 maggio 2018 trova piena applicazione la nuova normativa in materia di privacy che, come previsto dall'art. 99 del Regolamento UE 2016/679, è obbligatoria in tutti i suoi elementi e abroga espressamente la direttiva 95/46/CE.

La natura non tassativa delle indicazioni tracciate è peraltro fisiologica conseguenza dell'essenza stessa del Regolamento, fondato sul principio della accountability, in virtù del quale è il titolare del trattamento ad essere investito del compito (e della responsabilità) di garantire l'adempimento agli obblighi previsti dalle norme e l'efficacia della tutela predisposta, in un bilanciamento di discrezionalità di adempimenti e responsabilità per la verifica della loro efficacia. Obblighi che comprendono quelli di riesame ed aggiornamento costante di tutte le condizioni adottate nel proprio sistema di trattamento e protezione dei dati personali.

LA DISCIPLINA

Trattamento dei dati personali (art. 5)

Ai sensi dell'art. 5 del Regolamento i dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

Le finalità devono essere determinate, esplicite e legittime.

Anche i dati trattati devono essere adeguati, circoscritti e limitati tenendo conto della necessità e della finalità. Al trattamento deve essere garantita adeguata sicurezza.

La trasparenza implica che ai titolari dei dati deve essere garantita l'informazione, chiara, semplice e facilmente accessibile, delle modalità attraverso le quali avviene l'utilizzazione, la consultazione e il trattamento dei dati personali che li riguardano.

Del rispetto dei princìpi fissati dall'art. 5, della loro adeguatezza, aggiornamento e sicurezza è responsabile il titolare del trattamento.

Liceità del trattamento e consenso (art. 6)

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. n. 196/2003.

Elemento fondamentale della liceità del trattamento è il consenso.

Consenso (art. 7)

Ai sensi dell'art. 7 del Regolamento il consenso deve essere prestato in maniera chiara e semplice, in forma comprensibile e facilmente accessibile.

Il Regolamento non prevede obbligatoriamente la forma scritta per il consenso.

Tuttavia considerato che il titolare del trattamento, sempre ai sensi dell'art. 7, par. 1, è onerato di *"dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali",* è evidentemente raccomandata l'opportunità di provvedere all'acquisizione del consenso in forma scritta.

Deve essere chiaro anche il riconoscimento del diritto a revocare il proprio consenso in qualsiasi momento.
Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutti i requisiti indicati nel Regolamento (UE) 2016/679. In caso contrario è opportuno, prima di tale data, raccogliere nuovamente il consenso degli interessati secondo quanto previsto dalla novella normativa.

Consenso Obbligatorio
La prestazione del consenso deve essere tale da consentire la dimostrazione dell'effettività dei princìpi fissati dall'art. 7, rendendo chiaro ed inequivocabile: a) che l'interessato ha acconsentito al trattamento;
b) che l'interessato ha prestato il consenso nella piena consapevolezza della misura e delle modalità con le quali il trattamento avviene;
c) forma accessibile e linguaggio semplice ed inequivocabile;
d) l'indicazione dell'identità del titolare del trattamento dei dati;
e) la finalità del trattamento cui sono destinati i dati personali;
f) la specifica indicazione del diritto alla revoca del consenso;
g) la separazione tra i consensi prestati rispetto ai dati ed alle finalità di trattamento, laddove distinti.

Consenso facoltativo
Il trattamento è considerato lecito quando è necessario:

- nell'ambito di un contratto o ai fini della sua conclusione o esecuzione;
- per adempiere ad un obbligo legale;
- per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Ricorrendo una delle precedenti ipotesi, il consenso non è necessario ed è sufficiente la consegna dell'informativa (con ricevuta che attesti la presa visione da parte dell'interessato), che conferma così la centralità e fondamentalità della propria funzione nell'ambito del trattamento dei dati personali.
Si ricade in queste condizioni ed il trattamento dei dati – previa informativa – è lecito a prescindere dal consenso quando, ad esempio, i dati debbono essere acquisiti e trattati nell'ambito della gestione di un contratto e conseguente rapporto di lavoro, mandato professionale ed ogni attività fisiologicamente connessa (a mero titolo esemplificativo e non esaustivo: instaurazione e gestione del rapporto di lavoro; elaborazione prospetti paga; adempimenti dichiarativi in materia contributiva e fiscale; gestione di infortuni e malattia, etc.)

Categorie particolari di dati (art. 9)
Così come indicato all'art. 9 del Regolamento, il consenso all'acquisizione dei dati sensibili deve essere esplicito. Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

Per espressa previsione dell'art. 9, par. 2, lett. b) del Regolamento, il divieto al trattamento, altrimenti previsto per i dati c.d. "sensibili", non si applica ed il trattamento è considerato lecito quando è necessario per assolvere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

Informativa (artt. 12 – 14)

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Gli artt. 13 e 14 del Regolamento indicano le informazioni che devono essere fornite qualora i dati siano raccolti presso l'interessato (art. 13) o presso altri soggetti (art. 14).

L'informativa è un momento fondamentale del trattamento dati, ne caratterizza la fase iniziale ed accompagna ogni sua fase.

Assolve in concreto al principio di trasparenza effettiva, garantendo all'interessato la possibilità di conoscere, ad esempio, il periodo di conservazione dei dati e le modalità tecniche attraverso le quali questa avviene. Il contenuto dell'informativa, complesso e più completo di quella già nota, deve essere utile a rendere edotto il titolare circa tutti i diritti che gli sono riconosciuti dal Regolamento, tra i quali necessariamente:

- diritto di accesso ai dati (art. 15);
- diritto di rettifica (art. 16);
- diritto alla cancellazione (c.d. "diritto all'oblio", art. 17);
- diritto di limitazione del trattamento (art. 18);
- diritto alla portabilità dei dati (art. 20);
- diritto di opposizione (art. 21).

Registri delle attività di trattamento (art. 30)

Il registro dei trattamenti (art. 30 Reg.) è uno strumento fondamentale ai fini del monitoraggio degli adempimenti e della garanzia dei diritti previsti dal Regolamento n. 2016/679.

La sua previsione non è obbligatoria per il titolare del trattamento che occupi meno di 250 dipendenti.

L'obbligo prescinde dal requisito dimensionale nel caso in cui i dati oggetto del trattamento possano presentare un rischio per i diritti e le libertà degli interessati, il trattamento non sia occasionale o includano dati sensibili, genetici, biometrici, giudiziari, così come individuati dagli artt. 9 e 10 del Regolamento.

Adeguatezza delle misure adottate (artt. 24 – 26)

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.

Dette misure sono riesaminate e aggiornate qualora necessario; ciò implica anche la verifica e l'eventuale necessità di adeguamento degli strumenti (*hardware /* software) attraverso i quali il trattamento viene effettuato.
Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo, il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati (c.d. *"privacy by design"*).
Il titolare del trattamento attua misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi (c.d. *"privacy by default"*).

Valutazione d'impatto sulla protezione dati (artt. 35 – 36)
Sono obbligati alla valutazione d'impatto i titolari che debbano iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche, per le caratteristiche del trattamento o degli strumenti adottati per esso (ad esempio novità tecnologiche, finalità, natura dei dati). Quando la valutazione di impatto indica che il trattamento presenta un rischio elevato, prima di procedere al trattamento, il titolare è tenuto a consultare l'autorità di controllo.
Al di fuori di tali esigenze specifiche non è un adempimento standard riferibile all'attività di consulenza del lavoro.

Nomina responsabili esterni (art. 28)
Qualora un trattamento debba essere effettuato per conto del titolare, quest'ultimo ricorre unicamente a responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il citato trattamento soddisfi i requisiti del Regolamento (UE) e garantisca la tutela dei diritti dell'interessato (art.28).

Nomina autorizzati al trattamento
Pur non prevedendo espressamente la figura dell'incaricato del trattamento, il regolamento non ne esclude la presenza, in quanto fa riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 par. 10).
Tale figura è colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica e deve agire sotto la diretta autorità del titolare o del responsabile del trattamento.

Data Protection Officer (a**rt. 37 ss.)**
Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese "Data Protection Officer" – DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679.
La normativa non prevede tassativi requisiti per rivestire il ruolo di DPO. Il responsabile della protezione dei dati è designato, infatti, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'art. 39 del medesimo Regolamento (UE).

Non è obbligatorio per lo studio del singolo professionista, in quanto le attività principali dello stesso non consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

Data breach (art. 35)

Tutti i titolari del trattamento devono notificare all'autorità di controllo le violazioni di dati personali senza ingiustificato ritardo e, dove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, dovrà essere corredata dei motivi del ritardo (art.33).
Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica, con un linguaggio semplice e chiaro, la violazione all'interessato senza ingiustificato ritardo (art.34).

Sanzioni

All'art. 83 del Regolamento, par. 2, sono indicati i criteri che le autorità di controllo devono utilizzare per valutare sia l'opportunità di irrogare una sanzione amministrativa sia l'importo della stessa. Tali sanzioni devono essere in ogni caso effettive, proporzionate e dissuasive. Quasi tutti gli obblighi dei titolari e dei responsabili del trattamento sono classificati in base alla loro natura nelle disposizioni contenute all'articolo 83, paragrafi 4, 5 e 6. Il regolamento non fissa un importo specifico per ogni singola violazione, ma solo un massimale. Infatti, la violazione delle citate disposizioni è soggetta, a seconda delle diverse tipologie, a sanzioni amministrative pecuniarie fino a 10 o 20 milioni di euro o, per le imprese, fino al 2% o 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Il 4 Settembre 2018 è stato pubblicato in Gazzetta Ufficiale il D. Lgs. 10 Agosto 2018 n. 101 che armonizza l'ordinamento italiano al Regolamento (UE) n. 679/2016.

DATI ORDINE PROFESSIONALE

Ragione Sociale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**
Partita IVA	----------
Codice fiscale	80089990016
Sede legale	Via Stellone 5, 10126 Torino - TO
Contatti	- Tel: 0116634006 - Email: segreteria@opi.torino.it
Sito web	www.opi.torino.it
Attività economica	Ente pubblico non economico che agisce quale organo sussidiario dello Stato al fine di tutelare gli interessi pubblici, garantiti dall'ordinamento, connessi all'esercizio professionale; è finanziato esclusivamente con i contributi degli Iscritti, senza oneri per la finanza pubblica
Codici ATECO	• S. 94.12.10 - Attività di Federazioni e Consigli di Ordini e Collegi professionali
Rappresentante legale	Sciretti Massimiliano
Codice fiscale	SCRMSM71R17L219K
Contatti	sciretti.massimiliano@opi.torino.it

SEDI

Nome	**TO_ORDINE DELLE PROFESSIONI INFERMIERISTICHE DELLA PROVINCIA DI TORINO**
Tipo	- Legale - Amministrativa - Operativa
Indirizzo	Via Stellone 5, 10126 Torino - TO

NOMINE

Soggetto	**Studio Casapieri s.a.s.**, p.iva 07051740012
Contatti	
Nomina	**Responsabile del trattamento esterno** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Studio Triberti Colombo & Associati**, p.iva 10145950969
Contatti	
Nomina	**Responsabile del trattamento esterno** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**PA Digitale SpA**, p.iva 06628860964
Contatti	
Nomina	**Responsabile del trattamento esterno** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Dellacà Paola**
Contatti	paola.dellaca@opi.torino.it
Nomina	**Incaricato controllo accessi ai locali** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Nomina	**Incaricato del trattamento** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Delpero Fiorella**
Contatti	fiorella.delpero@opi.torino.it
Nomina	**Incaricato del trattamento** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Delpiano Laura**
Contatti	laura.delpiano@opi.torino.it
Nomina	**Incaricato controllo accessi ai locali** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Nomina	**Incaricato del trattamento** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Faenzi Cristina**
Contatti	faenzi.cristina@opi.torino.it
Nomina	**Responsabile del trattamento** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Fusaro Pasquale**
Contatti	dott.pfusaro@gmail.com
Nomina	**Responsabile del trattamento esterno** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Genipro Alberto**
Contatti	studiogenipro@gmail.com
Nomina	**Responsabile del trattamento esterno** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Lanzarone Salvatore**
Contatti	lanzarone.salvatore@opi.torino.it
Nomina	**Responsabile del trattamento** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Occhiena Massimo**
Contatti	massimo.occhiena@occhiena.it
Nomina	**Responsabile del trattamento esterno** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Soggetto	**Sciretti Massimiliano**, c.f. SCRMSM71R17L219K
Contatti	sciretti.massimiliano@opi.torino.it
Nomina	**Titolare del trattamento** Sede: TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

PARTNERS

Nominativo	**Studio Casapieri s.a.s.**
Tipo Partner	Partner/fornitore
Partita IVA	07051740012
Codice fiscale	
Indirizzo sede legale	Corso Francesco Ferrucci 77/10, 10138 Torino - TO
Contatti	segreteria@casapieri.it

Nominativo	**Studio Triberti Colombo & Associati**
Tipo Partner	Partner/fornitore
Partita IVA	10145950969
Codice fiscale	
Indirizzo sede legale	Via Giosuè Carducci 32, 20123 Milano - MI
Contatti	emanuela.glerean@tricol.it

Nominativo	**PA Digitale SpA**
Tipo Partner	Partner/fornitore
Partita IVA	06628860964
Codice fiscale	
Indirizzo sede legale	Via Leonardo Da Vinci 13, 26854 Pieve Fissiraga - LO
Contatti	protocollo.pec.padigitalespa@legalmail.it

Nominativo	**Occhiena Massimo**
Tipo Partner	Partner/fornitore
Partita IVA	06845410965
Codice fiscale	CCHMSM68L03L219C
Indirizzo residenza	Via Alfonso Lamarmora 6, 10121 Torino - TO
Contatti	massimo.occhiena@occhiena.it

Nominativo	**Fusaro Pasquale**
Tipo Partner	Partner/fornitore
Partita IVA	06563950010
Codice fiscale	FSRPQL63D12A893H
Indirizzo residenza	Via Rivalba 9/A, 10090 - TO
Contatti	dott.pfusaro@gmail.com

Nominativo	**Genipro Alberto**
Tipo Partner	Partner/fornitore
Partita IVA	01955320021
Codice fiscale	GNPLRT65R20L750E
Indirizzo residenza	Via E. Foa 70, 13100 Vercelli - VC
Contatti	- Email: studiogenipro@gmail.com

ARCHIVI INFORMATICI

Nome	**TO_Iscritti/Albo**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Faenzi Cristina, c.f. FNZCST66H57L219Y Delpero Fiorella, c.f. DLPFLL62M44L219X Delpiano Laura, c.f. DLPLRA63A43L219E Dellacà Paola, c.f. DLLPLA75C49L219B Sciretti Massimiliano, c.f. SCRMSM71R17L219K
Software utilizzati	- Microsoft Windows 10

Nome	**TO_Contabilità**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Delpero Fiorella, c.f. DLPFLL62M44L219X Delpiano Laura, c.f. DLPLRA63A43L219E Sciretti Massimiliano, c.f. SCRMSM71R17L219K Dellacà Paola, c.f. DLLPLA75C49L219B Lanzarone Salvatore, LNZSVT77T31L219K
Software utilizzati	- URBI SMART gestionale web

Nome	**TO_Legali**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K Faenzi Cristina, c.f. FNZCST66H57L219Y Delpero Fiorella, c.f. DLPFLL62M44L219X Delpiano Laura, c.f. DLPLRA63A43L219E Dellacà Paola, c.f. DLLPLA75C49L219B
Software utilizzati	- Windows

Nome	**TO_Commissioni**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Faenzi Cristina, c.f. FNZCST66H57L219Y Delpero Fiorella, c.f. DLPFLL62M44L219X Delpiano Laura, c.f. DLPLRA63A43L219E Dellacà Paola, c.f. DLLPLA75C49L219B
Software utilizzati	- Windows

Nome	**TO_Sicurezza e Privacy**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Delpero Fiorella, c.f. DLPFLL62M44L219X Delpiano Laura, c.f. DLPLRA63A43L219E Sciretti Massimiliano, c.f. SCRMSM71R17L219K Dellacà Paola, c.f. DLLPLA75C49L219B
Software utilizzati	- Windows

Nome	**Formazione ECM**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K Delpero Fiorella, c.f. DLPFLL62M44L219X Delpiano Laura, c.f. DLPLRA63A43L219E Dellacà Paola, c.f. DLLPLA75C49L219B
Software utilizzati	Portale per la formazione in Sanità della Regione Piemonte

Nome	**Personale Dipendente**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K Faenzi Cristina, c.f. FNZCST66H57L219Y
Software utilizzati	- Windows

Ordine delle Professioni Infermieristiche di Torino

ORGANIGRAMMA GDPR

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

SEDE LEGALE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

Di seguito, è riportato l'organigramma con le funzioni nominate per la gestione della protezione del trattamento dati personali:

SEDE TO_ORDINE DELLE PROFESSIONI INFERMIERISTICHE DELLA PROVINCIA DI TORINO

Titolare del trattamento:	**Sciretti Massimiliano**	Data nomina: 21 giugno 2018 (delibera 213/18)

Responsabili interni del trattamento:	**Faenzi Cristina**	Data nomina: 21 giugno 2018 (delibera 213/18)
	Lanzarone Salvatore	Data nomina: 21 giugno 2018 (delibera 213/18)

Responsabili esterni del trattamento:	**Studio Casapieri s.a.s.**	Data nomina: 13/12/2018
	Studio Triberti Colombo & Associati	Data nomina: 13/12/2018
	PA Digitale SpA	Data nomina: 13/12/2018
	Fusaro Pasquale	Data nomina: 13/12/2018
	Colla Susanna responsabile RSPP	Data nomina: 13/12/2018
	Genipro Alberto	Data nomina: 02/08/2018
	Occhiena Massimo **ITALRISCOSSIONI** **FNOPI** **ANAGRAFE TRIBUTARIA** **DIPARTIMENTO DELLA FUNZIONE PUBBLICA** **Regione Piemonte**	Data nomina: 25/01/2016 Data nomina: 16/11/2017 Albo nazionale istituito nel 2005 Dm del 17-09-1999 Dl. 165/2001 Database regionale istituito nel 2008

Incaricato controllo accessi ai locali:	**Dellacà Paola**	Data nomina: 01/03/2007
	Delpiano Laura	Data nomina: 01/03/2007

Incaricato del trattamento:	**Dellacà Paola**	Data nomina: 01/03/2007
	Delpero Fiorella	Data nomina: 01/03/2007
	Delpiano Laura	Data nomina: 01/03/2007

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Iscritti/Albo
SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

Responsabile trattamento dati	Cognome	Faenzi
	Nome	Cristina

TRATTAMENTO: TO_Iscritti/Albo
Scheda creata in data: 06/12/2018

Struttura	• Segreteria

Personale coinvolto	
Persone autorizzate	Faenzi Cristina (Consigliere Segretario) • Inserimento • Consultazione • Modifica • Cancellazione Delpero Fiorella (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Delpiano Laura (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Dellacà Paola (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Sciretti Massimiliano (Rappresentante legale)

Partners - Responsabili esterni	
Altro	FNOPI – ITALRISCOSSIONI – ANAGRAFE TRIBUTARIA – ECM PIEMONTE – PER LA PA

Processo di trattamento	
Descrizione	Gestione anagrafe iscritti, rilascio certificati, accertamento/iscrizione.
Fonte dei dati personali	Forniti dagli Iscritti Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Adempimenti connessi con la gestione degli iscritti all'Ordine Professionale
Tipo di dati personali	Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Particolari (sensibili) Personali Codice fiscale
Categorie di interessati	Soggetti o organismi pubblici Enti Iscritti all'Ordine Professionale
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Associazioni ed enti locali Altre amministrazioni pubbliche Enti previdenziali ed assistenziali Enti pubblici non economici Ordini e Collegi professionali Organismi per i Collegi professionali Organismi sanitari, personale medico e paramedico Persone autorizzate
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Quotidiano
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale Windows
Archiviazione	Armadio chiuso a chiave Armadi senza serratura Cassaforte

Strutture informatiche di archiviazione	
TO_Iscritti/Albo	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Personale con diritti di accesso	Faenzi Cristina (Consigliere Segretario) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo) Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale)
Note	
Software utilizzati	- Microsoft Windows 10
Strutture informatiche di backup	
TO_Iscritti/Albo	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Faenzi Cristina (Consigliere Segretario) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo) Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale)
Note	
Software utilizzati	- Microsoft Windows 10

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Contabilità

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

Responsabile trattamento dati	Cognome	Lanzarone
	Nome	Salvatore

TRATTAMENTO: TO_Contabilità
Scheda creata in data: 06/12/2018

Struttura	• Segreteria

Personale coinvolto	
Persone autorizzate	Delpiano Laura (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Sciretti Massimiliano (Rappresentante legale) • Consultazione Lanzarone Salvatore (Tesoriere) • Consultazione
Partners - Responsabili esterni	Studio Triberti Colombo & Associati, p.iva 10145950969 (Outsourcer) • Comunicazione • Conservazione • Consultazione • Elaborazione • Inserimento • Raccolta PA Digitale SpA, p.iva 06628860964 (Outsourcer) • Conservazione • Consultazione • Raccolta

Altro	

Processo di trattamento	
Descrizione	Adempimenti fiscali, dichiarazione IVA, bilanci, fatture acquisto, polizze. assicurative a tutela dei consiglieri, riscossione tasse, ecc.
Fonte dei dati personali	Forniti da terzi Forniti dagli Iscritti Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Adempimento di obblighi di legge connessi a rapporti commerciali Adempimento di obblighi fiscali o contabili Gestione contabile o di tesoreria Gestione dei fornitori (contratti, ordini, arrivi, fatture) Assicurazione
Tipo di dati personali	Dati assicurativi Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Categorie di interessati	Consulenti e liberi professionisti, anche in forma associata Enti Iscritti all'Ordine Professionale
Categorie di destinatari	Enti previdenziali ed assistenziali Enti pubblici economici Fornitori di servizi amministrativi e contabili Imprese di assicurazione
Informativa	Non necessaria
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Quotidiano
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Armadio chiuso a chiave Armadi senza serratura Cassaforte
Strutture informatiche di archiviazione	
TO_Contabilità	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Personale con diritti di accesso	Delpiano Laura (Amministrativo) Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Lanzarone Salvatore (Consigliere Tesoriere)
Note	
Software utilizzati	URBISMART
Strutture informatiche di backup	
TO_Contabilità	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino

Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Dellacà Paola (Amministrativo) Lanzarone Salvatore (Consigliere Tesoriere)
Note	
Software utilizzati	- Windows

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - L'impianto elettrico è certificato ed a norma - Viene eseguita opportuna manutenzione - Le password sono costituite da almeno otto caratteri alfanumerici - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita una regolare formazione del personale

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Legali

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 06/12/2018

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

Responsabile trattamento dati	Cognome	Faenzi
	Nome	Cristina

TRATTAMENTO: TO_Legali
Scheda creata in data: 06/12/2018
Ultimo aggiornamento avvenuto in data: 06/12/2018

Struttura	

Personale coinvolto	
Persone autorizzate	Faenzi Cristina (Consigliere Segretario) • Conservazione • Consultazione • Raccolta Delpero Fiorella (Amministrativo) • Conservazione • Consultazione • Raccolta Delpiano Laura (Amministrativo) • Conservazione • Consultazione • Raccolta Sciretti Massimiliano (Rappresentante legale) • Conservazione • Consultazione • Raccolta Dellacà Paola (Amministrativo) • Conservazione • Consultazione • Raccolta

Partners - Responsabili esterni	Occhiena Massimo (Outsourcer) • Conservazione • Consultazione • Diffusione • Elaborazione • Inserimento • Modifica • Raccolta Bossi Marcello (Outsourcer) • Conservazione • Consultazione • Diffusione • Elaborazione • Inserimento • Modifica • Raccolta
Altro	

Processo di trattamento	
Descrizione	Consulenze legali
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa Legge
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legge Legittimo interesse
Finalità del trattamento	Acquisizione di prove Adempimenti connessi con la gestione degli iscritti all'Ordine Professionale Attività di consulenza
Tipo di dati personali	Giudiziari Personali
Categorie di interessati	Iscritti in albi ed elenchi
Categorie di destinatari	Ordini e collegi professionali Servizi di giustizia e di polizia Uffici giudiziari Studi legali Enti previdenziali ed assistenziali Enti pubblici non economici
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Mensile
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Armadio chiuso a chiave Cassaforte Armadi senza serratura

Strutture informatiche di archiviazione	
TO_Legali	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Faenzi Cristina, c.f. FNZCST66H57L219Y (Consigliere Segretario) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	- Windows
Strutture informatiche di backup	
TO_Legali	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Faenzi Cristina (Consigliere Segretario) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	- Windows

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - L'impianto elettrico è certificato ed a norma - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale - Le password sono costituite da almeno otto caratteri alfanumerici - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Commissioni

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

Responsabile trattamento dati	Cognome	Faenzi
	Nome	Cristina

TRATTAMENTO: TO_Commissioni
Scheda creata in data: 06/12/2018

Struttura	• Accettazione

Personale coinvolto	
Persone autorizzate	Faenzi Cristina (Consigliere Segretario) • Inserimento • Consultazione • Modifica • Cancellazione Delpero Fiorella (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Delpiano Laura (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Dellacà Paola (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione

Partners - Responsabili esterni	
Altro	

Processo di trattamento	
Descrizione	Designazione rappresentanti commissioni varie
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legittimo interesse
Finalità del trattamento	Adempimenti connessi con la gestione degli iscritti all'Ordine Professionale
Tipo di dati personali	Codice fiscale Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati finanziari
Categorie di interessati	Componenti Consiglio dell'Ordine Professionale
Categorie di destinatari	Enti pubblici non economici Ordini e collegi professionali
Informativa	Non necessaria
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Mensile
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Armadio chiuso a chiave Cassaforte Armadi senza serratura
Strutture informatiche di archiviazione	
TO_Commissioni	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Personale con diritti di accesso	Faenzi Cristina (Consigliere Segretario) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	- Windows
Strutture informatiche di backup	
TO_Commissioni	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni

Personale con diritti di accesso	Faenzi Cristina (Consigliere Segretario) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	- Windows

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita una regolare formazione del personale - Viene eseguita opportuna manutenzione

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Sicurezza e Privacy

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 10/01/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

Responsabile trattamento dati	Cognome	Faenzi
	Nome	Cristina

TRATTAMENTO: TO_Sicurezza e Privacy
Scheda creata in data: 06/12/2018
Ultimo aggiornamento avvenuto in data: 10/01/2019

Struttura	• Uff. Presidente • Segreteria

Personale coinvolto	
Persone autorizzate	Faenzi Cristina (Consigliere Segretario) • Conservazione • Consultazione • Raccolta Delpero Fiorella (Amministrativo) • Conservazione • Consultazione • Raccolta Delpiano Laura (Amministrativo) • Conservazione • Consultazione • Raccolta Sciretti Massimiliano (Rappresentante legale) • Conservazione • Consultazione • Raccolta Dellacà Paola (Amministrativo) • Conservazione • Consultazione • Raccolta

Partners - Responsabili esterni	Genipro Alberto (Outsourcer) • Cancellazione • Comunicazione • Conservazione • Consultazione • Elaborazione • Inserimento • Modifica • Raccolta
Altro	

Processo di trattamento	
Descrizione	Documento di valutazione dei rischi aziendali e documento relativo al trattamento dei dati
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Gestione l. 81/2008 Trattamento dei dati
Tipo di dati personali	Codice fiscale Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Particolari (sensibili)
Categorie di interessati	Dott.ssa Susanna Colla Collaboratori Iscritti in albi ed elenchi
Categorie di destinatari	Datore di lavoro
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Mensile
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Windows
Archiviazione	Armadio chiuso a chiave Cassaforte Armadi senza serratura
Strutture informatiche di archiviazione	
TO_Sicurezza e Privacy	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Personale con diritti di accesso	Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo)

	Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	- Windows
Strutture informatiche di backup	
TO_Sicurezza e Privacy	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	- Windows

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Formazione ECM

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

TRATTAMENTO: TO_RG_Formazione ECM
Scheda creata in data: 12/01/2019
Ultimo aggiornamento avvenuto in data: 12/01/2019

Struttura	• Accettazione • Contabilità • Uff. Presidente

Personale coinvolto	
Persone autorizzate	Sciretti Massimiliano (Rappresentante legale) • Inserimento • Consultazione • Modifica • Cancellazione Delpero Fiorella (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Delpiano Laura (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione Dellacà Paola (Amministrativo) • Inserimento • Consultazione • Modifica • Cancellazione
Partners - Responsabili esterni	C.S.I. Piemonte - 01995120019 N.B.S. s.r.l. - 01517290670

Altro	

Processo di trattamento	
Descrizione	Sistema qualità ECM Piemonte, arruolamento alla formazione iscritti, gestione dei corsi e certificazione avvenuta formazione
Fonte dei dati personali	Forniti dagli Iscritti Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legittimo interesse
Finalità del trattamento	Gestione formazione ECM
Tipo di dati personali	Codice fiscale Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)
Categorie di interessati	Iscritti all'Ordine Professionale Formatori Docenti
Categorie di destinatari	ECM Piemonte
Informativa	Non necessaria
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Quindicinale
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Scaffalature
Strutture informatiche di archiviazione	
Strutture informatiche di backup	
Formazione ECM	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Delpero Fiorella (Amministrativo) Delpiano Laura (Amministrativo) Dellacà Paola (Amministrativo)
Note	
Software utilizzati	data base Regione Piemonte

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee

Ordine delle Professioni Infermieristiche di Torino

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

REGISTRO	Personale dipendente

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Sciretti
	Nome	Massimiliano

TRATTAMENTO: TO_RG_Personale dipendente
Scheda creata in data: 12/01/2019
Ultimo aggiornamento avvenuto in data: 12/01/2019

Struttura	• Uff. Presidente

Personale coinvolto	
Persone autorizzate	Sciretti Massimiliano (Rappresentante legale) • Inserimento • Consultazione • Modifica • Cancellazione
Partners - Responsabili esterni	Studio Casapieri s.a.s., p.iva 07051740012 (Outsourcer) • Inserimento • Consultazione • Modifica • Cancellazione Fusaro Pasquale (Outsourcer) • Consultazione • Inserimento • Modifica • Cancellazione
Altro	

Processo di trattamento	
Descrizione	Gestione dei dipendenti
Fonte dei dati personali	Raccolti direttamente Forniti da terzi
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Legittimo interesse Consenso
Finalità del trattamento	Gestione del personale
Tipo di dati personali	Codice fiscale Dati assicurativi

	Adesione a sindacati o organizzazioni a carattere sindacale Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Dati relativi alla prestazione lavorativa Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)
Categorie di interessati	Componenti Consiglio dell'Ordine Professionale Consulenti e liberi professionisti, anche in forma associata Dipendenti
Categorie di destinatari	
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Mensile
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	Armadio chiuso a chiave
Strutture informatiche di archiviazione	
Strutture informatiche di backup	
Personale Dipendente	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K (Rappresentante legale) Fusaro Pasquale (Outsourcer) Colla Susanna (Outsourcer)
Note	
Software utilizzati	- Windows

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Antivirus
  Estintori
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Viene eseguita una regolare formazione del personale

Ordine delle Professioni Infermieristiche di Torino

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

TITOLARE	Sciretti Massimiliano

SEDE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(*1 ≤ *LR* ≤ 3*)*
Medio - basso	*(*4 ≤ *LR* ≤ 6*)*
Rilevante	*(*8 ≤ *LR* ≤ 12*)*
Alto	*(*15 ≤ *LR* ≤ 25*)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala

6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – valutazione del rischio normalizzato

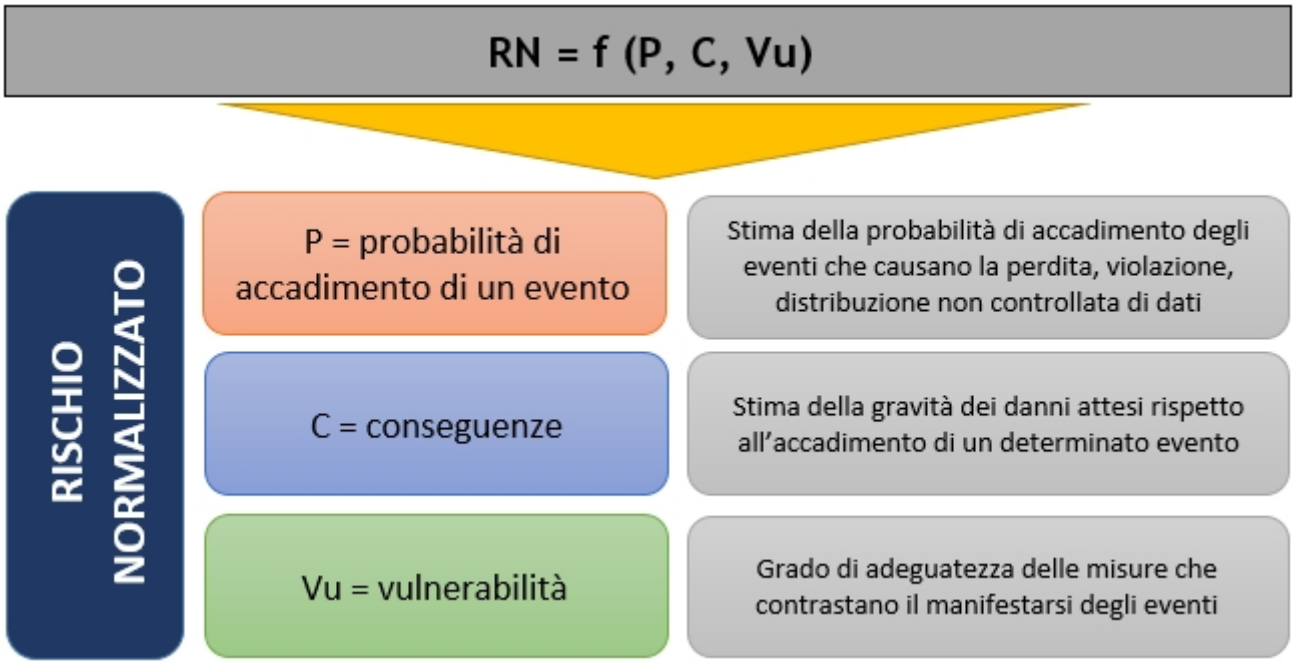
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

P = probabilità
C = conseguenze generate dall'evento
V = vulnerabilità rispetto al grado di adeguatezza delle misure



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**Quasi certo**

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	**Valori di riferimento**
Molto basso	*(1 ≤ Ri ≤ 2)*
Basso	*(3 ≤ Ri ≤ 4)*
Rilevante	*(6 ≤ Ri ≤ 9)*
Alto	*(12 ≤ Ri ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità** (Vu) è associato un indice numerico rappresentato nella seguente tabella:

	VULNERABILITA'	Valore
1	**Adeguate**	**0,25**
2	**Parzialmente adeguate**	**0,5**
3	**Inadeguate**	**1**

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- TO_Iscritti/Albo
- TO_RG_Personale dipendente

TO_Iscritti/Albo

Struttura	• Segreteria

Personale coinvolto	
Titolare del trattamento	Sciretti Massimiliano
Persone autorizzate	Faenzi Cristina • Inserimento • Consultazione • Modifica • Cancellazione Delpero Fiorella • Inserimento • Consultazione • Modifica • Cancellazione Delpiano Laura • Inserimento • Consultazione • Modifica • Cancellazione Dellacà Paola • Inserimento • Consultazione • Modifica • Cancellazione Sciretti Massimiliano, c.f. SCRMSM71R17L219K
Partners - Responsabili esterni	
Altro	

Processo di trattamento	
Descrizione	Gestione anagrafe iscritti, rilascio certificati, accertamento/iscrizione.
Fonte dei dati personali	Forniti dagli Iscritti Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Informativa
Base giuridica per il trattamento	

per dati particolari (art. 9 GDPR)	
Finalità del trattamento	Adempimenti connessi con la gestione degli iscritti all'Ordine Professionale
Tipo di dati personali	Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) Particolari (sensibili) Personali Codice fiscale
Categorie di interessati	Soggetti o organismi pubblici Enti Iscritti all'Ordine Professionale
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Associazioni ed enti locali Altre amministrazioni pubbliche Enti previdenziali ed assistenziali Enti pubblici non economici Ordini e collegi professionali Organismi per i collegi professionali Organismi sanitari, personale medico e paramedico Persone autorizzate
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Quotidiano
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale Windows
Strutture informatiche di archiviazione	
TO_Iscritti/Albo	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Personale con diritti di accesso	Faenzi Cristina Delpero Fiorella Delpiano Laura Dellacà Paola Sciretti Massimiliano, c.f. SCRMSM71R17L219K
Software utilizzati	- Microsoft Windows 10
Strutture informatiche di backup	
TO_Iscritti/Albo	Struttura interna
Sede di riferimento	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino
Frequenza di backup	1 giorni
Tempo di storicizzazione	1 giorni
Personale con diritti di accesso	Faenzi Cristina Delpero Fiorella Delpiano Laura Dellacà Paola Sciretti Massimiliano, c.f. SCRMSM71R17L219K

Note	
Software utilizzati	- Microsoft Windows 10

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Antivirus	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Estintori	• Agenti fisici (incendio, attacchi esterni)	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate

Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante

VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**

TO_RG_Personale dipendente

Processo di trattamento	
Descrizione	Gestione dei dipendenti
Finalità del trattamento	Gestione del personale
Tipo di dati personali	Codice fiscale Dati assicurativi Adesione a sindacati o organizzazioni a carattere sindacale Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Dati relativi alla prestazione lavorativa Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)
Tipologia di trattamento	
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Antivirus - Estintori - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Sono gestiti i back up - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Viene eseguita una regolare formazione del personale

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Antivirus	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Estintori	• Agenti fisici (incendio, attacchi esterni)	Adeguate

Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono utilizzati software antivirus e anti intrusione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Viene eseguita una regolare formazione del personale	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)
RISCHI
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**

Ordine delle Professioni Infermieristiche di Torino

VALUTAZIONE ARCHIVI INFORMATICI

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

SEDE LEGALE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

VALUTAZIONE ARCHIVI INFORMATICI

Di seguito, è riportata la valutazione degli archivi informatici in dotazione all'organizzazione.
L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

RISULTATI

Nome	TO_Iscritti/Albo
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Faenzi Cristina Delpero Fiorella Delpiano Laura Dellacà Paola Sciretti Massimiliano, c.f. SCRMSM71R17L219K
Note	
Software utilizzati	• Microsoft Windows 10

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		

VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)
RISCHI
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO
Agenti fisici (incendio, allagamento, attacchi esterni)
RISCHI
• Perdita • Distruzione non autorizzata

VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale

Nome	TO_Contabilità
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Delpero Fiorella Delpiano Laura Sciretti Massimiliano, c.f. SCRMSM71R17L219K Dellacà Paola Lanzarone Salvatore
Note	
Software utilizzati	• Windows

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale

Nome	TO_Legali
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K Faenzi Cristina Delpero Fiorella Delpiano Laura Dellacà Paola
Note	
Software utilizzati	• Windows

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • L'impianto elettrico è certificato ed a norma • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale • Le password sono costituite da almeno otto caratteri alfanumerici • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee

Nome	TO_Commissioni
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Faenzi Cristina Delpero Fiorella Delpiano Laura Dellacà Paola
Note	
Software utilizzati	• Windows

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita una regolare formazione del personale • Viene eseguita opportuna manutenzione

Nome	TO_Sicurezza e Privacy
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Delpero Fiorella Delpiano Laura Sciretti Massimiliano, c.f. SCRMSM71R17L219K Dellacà Paola
Note	
Software utilizzati	• Windows

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)
RISCHI
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
VALUTAZIONE RISCHIO

Probabilità	Conseguenza	Livello di rischio
Poco probabile	Limitate	Medio-basso

PERICOLO
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)
RISCHI
• Perdita • Distruzione non autorizzata • Modifica non autorizzata
VALUTAZIONE RISCHIO

Probabilità	Conseguenza	Livello di rischio
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale

Nome	Formazione ECM
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K Delpero Fiorella Delpiano Laura Dellacà Paola
Note	
Software utilizzati	• Windows

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee

Nome	**Personale Dipendente**
Tipo Struttura	Interna
Sede	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino (Torino)
Personale con diritti di accesso	Sciretti Massimiliano, c.f. SCRMSM71R17L219K
Note	
Software utilizzati	• Windows

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)

RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Antivirus • Estintori • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee • Sono gestiti i back up • Sono utilizzati software antivirus e anti intrusione • Viene eseguita opportuna manutenzione • Viene eseguita una regolare formazione del personale

Ordine delle Professioni Infermieristiche di Torino

ISTRUZIONI OPERATIVE

Ordine professionale	**OPI TO_Ordine delle Professioni Infermieristiche della Provincia di Torino**

SEDE LEGALE	TO_Ordine delle Professioni Infermieristiche della Provincia di Torino Via Stellone 5, 10126 Torino - TO

Data revisione: 12/01/2019

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

PREMESSA
L'utilizzo delle risorse informatiche e telematiche dell'Ordine Professionale deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. L'Ordine delle Professioni Infermieristiche della Provincia di Torino ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER
Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna**.**

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere all'Ordine Professionale, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dell'Ordine Professionale, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività dell'Ordine Professionale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici dell'Ordine Professionale*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* dell'Ordine delle Professioni Infermieristiche della Provincia di Torino**.** L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ordine Professionale a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici dell'Ordine Professionale*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici dell'Ordine Professionale***.**

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici dell'Ordine Professionale* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il *Responsabile dei sistemi informatici dell'Ordine Professionale* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite da**l** *Responsabile dei sistemi informatici dell'Ordine Professionale*.

È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici dell'Ordine Professionale. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici dell'Ordine Professionale*, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Consiglio Direttivo o al *Responsabile dei sistemi informatici.*

UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici dell'Ordine Professionale* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in sede, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Ordine Professionale all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica dell'Ordine Professionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per Ordine delle Professioni Infermieristiche della Provincia di Torino deve essere visionata od autorizzata dal Responsabile del Trattamento, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'Ordine Professionale "know how" tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del Trattamento.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno dell'Ordine delle Professioni Infermieristiche della Provincia di Torino è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici dell'Ordine Professionale*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento dell'Ordine Professionale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici dell'Ordine Professionale*.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA DELL'ORDINE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Consiglio Direttivo.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (data breach) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per "Violazione di dati" si intende 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 (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;

violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;

violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

Rischio assente: la notifica al Garante non è obbligatoria.

Rischio presente: è necessaria la notifica al Garante.

Rischio elevato: In presenza di rischi “elevati”, è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l’acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

riguardare categorie particolari di dati personali;

comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

comportare rischi imminenti e con un’elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

DEFINIZIONI
Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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;

Violazione dei dati personali: 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.

ADEMPIMENTI
Ciascun incaricato del trattamento deve:

rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;

rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;

utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'Ordine Professionale;

rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;

segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;

accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;

in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;

mantenere riservate le proprie credenziali di autenticazione;

svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;

raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di

studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Ordine Professionale di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente

autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

Non deve mai essere disattivato;

Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;

Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

• prima della riconsegna, rimuovere eventuali file ivi elaborati;

• quando il PC portatile è nei locali dell'Ordine Professionale, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;

• quando il PC portatile è all'esterno dell'Ordine Professionale, evitare di lasciarlo incustodito;

• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;

• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi dell'Ordine Professionale;

• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;

• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

• tutela l'utilizzatore ed in generale l'Ordine Professionale da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;

• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;

• è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

• devono essere lunghe almeno otto caratteri;

• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;

• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;

• non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

• Almeno ogni 3 mesi è obbligatorio cambiare la password;

• Ogni password ricevuta va modificata al primo utilizzo;

• La password venga conservata in un luogo sicuro;

• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;

• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle personale del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

• Non utilizzare sul PC dispositivi personali, o comunque non dell'Ordine Professionale, quali lettori dispositivi di memorizzazione dei dati;

• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete dell'Ordine Professionale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;

• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;

• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

Gestione posta elettronica dell'Ordine Professionale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Ordine Professionale e in stretta connessione con l'effettiva

attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'Ordine Professionale e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;

• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;

• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

• l'indirizzo del destinatario sia stato correttamente digitato,

• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;

• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

Gestione del salvataggio dei dati
Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

Gestione dei supporti rimovibili
I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Informatico. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

Gestione protezione dai virus informatici
Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Ordine Professionale è stato installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile.

L'antivirus dell'Ordine Professionale non deve mai essere disattivato o sostituito con altro antivirus

non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie.

Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;

• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:

• in nessun caso è concesso l'accesso a documentazione contenente dati personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;

• la documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;

• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i trattamenti previsti;

• i supporti devono essere archiviati in ambiente ad accesso controllato;

• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);

• il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro;

• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;

• l'accesso fuori orario lavorativo a documenti contenti dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;

• la distruzione di documenti contenenti dati personali deve essere operata, ove possibile, direttamente dal personale incaricato;

• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;

• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

• è severamente vietato utilizzare documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;

• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;

• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;

• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili e su indicazione dell'Amministratore di sistema;

• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.

• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.

• Per effettuare operazioni di manutenzione sui database dell'Ordine Professionale che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.

• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;

• È necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.

• Tutti i dati personali contenuti nei data base devono essere protetti da password;

• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;

o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.

• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso,

alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;

• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;

• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;

• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;

• È assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dall'Ordine Professionale, se non previa espressa comunicazione scritta;

• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

NON OSSERVANZA DELLA NORMATIVA DELL'ORDINE PROFESSIONALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Consiglio Direttivo.

Il presente Regolamento è soggetto a revisione con frequenza annuale.