Normativa di riferimento:

- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101
- Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (GDPR – General Data Protection Regulamentation), nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente modello.

ORDINE DELLE PROFESSIONI INFERMIERISTICHE DELLA PROVINCIA DI SIENA

Viale Europa 31, Cap. 53100 SIENA (SI)

Telefono: 0577281160

E-mail: info@opisiena.it

PEC: siena@cert.ordine-opi.it

Codice fiscale: 80009660525

Data	**Per approvazione** **Il Presidente**
21.05.2026	

Stato delle revisioni

Rev.	**Del**	**Descrizione**
0	28.05.2021	Prima emissione
01	22.04.2022	Aggiornamento anno 2022
02	21.05.2026	Aggiornamento anno 2026

Sommario

1 PREMESSA

Scopo del presente documento è quello di delineare il quadro delle misure adottate per il trattamento dei dati personali, dall' Ordine delle professioni infermieristiche di Siena.

Il Regolamento (UE) 2016/679 "General Data Protection Regulation" (GDPR) si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (articolo 2).

Non sono ricompresi nel campo di applicazione del Regolamento i trattamenti relativi ai dati che riguardano le persone giuridiche, gli enti e le associazioni.

La tutela rimane pertanto assicurata solo per i dati che riguardano le persone fisiche.

Gli Ordini professionali sono qualificabili come **enti pubblici non economici** che, nello svolgimento dei compiti istituzionali, trattano su larga scala dati personali, tra cui anche dati sensibili e giudiziari.

Il Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 noto anche come GDPR (General Data Protection Regulamentation), non prevede, come invece faceva il Codice della privacy, una distinzione tra condizioni di liceità applicabili a titolari del trattamento che fossero soggetti privati e condizioni valide per i titolari soggetti pubblici, cosicché l'istituto del consenso non costituisce più l'elemento distintivo tra titolari privati e titolari pubblici.

Infine, per una corretta analisi dei trattamenti effettuati dagli Ordini, vale ricordare preliminarmente che tali trattamenti sono posti in essere per l'esercizio delle funzioni e dei compiti attribuiti, in via istituzionale, agli Ordini stessi.

In particolare, i trattamenti effettuati nel detto esercizio di funzioni e compiti istituzionali sono volti a verificare, nei limiti necessari e proporzionali, il regolare espletamento delle attività normative e contrattuali da parte degli interessati.

Nota: il presente modello organizzativo è stato redatto sulla base delle indicazioni fornite dal Titolare del trattamento dei dati.

Ogni variazione, nella gestione del flusso dei dati, comporta la revisione del modello.

Il Modello Organizzativo è soggetto, inoltre, a verifica di adeguatezza annuale *che comprende la revisione del documento con l'inserimento delle modifiche necessarie, la registrazione della data di aggiornamento e la sottoscrizione da parte del titolare del trattamento del documento per l'adozione del nuovo documento di gestione organizzativa.*

2 SCOPO DEL PRESENTE MODELLO ORGANIZZATIVO

Lo scopo del presente documento e di quelli ad esso collegati è definire il Modello Organizzativo Privacy, ovvero individuare le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dall'ente, ai sensi del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (Codice della Privacy), come modificato dal D.Lgs. 10 agosto 2018, n. 101 e del Regolamento (UE) del Parlamento Europeo e del Consiglio del 27 aprile 2016, n. 679 (GDPR – General Data Protection Regulation), nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente documentazione.

In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del "Codice della Privacy" e del "GDPR", anche con riferimento alle decisioni e ai provvedimenti emessi dal Garante Europeo della Protezione dei Dati e dall'Autorità Garante Nazionale per la protezione dei dati personali.

3 PRINCIPALI DEFINIZIONI

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
L'articolo 4 del GDPR definisce "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.

Per trattamento si intende qualsiasi operazione compiuta ed applicata a dati personali.

Titolare del trattamento
Ai sensi dell'articolo 4 del GDPR, il "titolare del trattamento" è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'UE o dei suoi Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'UE o dei suoi Stati membri.

Il titolare del trattamento è l'entità che determina le finalità e i mezzi del trattamento di dati personali: *OPI Siena nella persona del suo Presidente: il Dott. Francesco D'Ambrosio.*

Responsabile del Trattamento:
Secondo l'articolo 4 del GDPR, il "responsabile del trattamento" è la persona fisica o giuridica, la pubblica amministrazione oppure l'ente che elabora i dati personali per conto del titolare del trattamento.
Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
Ai sensi del GDPR chiunque, all'interno di una organizzazione, effettui operazioni di trattamento è *"persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare".*
Quando il soggetto a cui è demandato in tutto o in parte il trattamento di dati personali da parte del titolare è un soggetto esterno all'organizzazione di quest'ultimo, la nomina dello stesso come responsabile del trattamento non solo è necessaria, ma deve avvenire per iscritto in virtù di apposito contratto o previsione incluso in un contratto tra il titolare ed il responsabile stesso.
In forza del menzionato contratto, il responsabile del trattamento si obbliga a:

- trattare i dati personali solo sulla base di un'istruzione documentata del titolare del trattamento;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure richieste dall'articolo 32 del GDPR, ovvero le misure tecniche e organizzative necessarie al fine di garantire un livello di sicurezza adeguato al rischio;

- rispettare tutte le condizioni previste per l'eventuale nomina di un sub-responsabile;
- assistere il titolare del trattamento con misure tecniche e organizzative adeguate, e tenuto conto della natura del trattamento, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi in materia di tutela della sicurezza dei dati;
- su indicazione del titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento o dopo che è terminato il tempo di conservazione previsto dal titolare e conforme alle prescrizioni del regolamento;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei suoi obblighi;
- contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da lui incaricato;
- informare immediatamente il titolare del trattamento qualora ritenga che un'istruzione del titolare violi il Regolamento o altre disposizioni nazionali o di diritto europeo relative alla protezione dei dati.

Il responsabile ha la possibilità di nominare dei sub-responsabili del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare; è previsto che il responsabile del trattamento possa ricorrere ad un altro responsabile solo previa autorizzazione scritta (che può essere, però, sia specifica che generale) del titolare del trattamento.

Il responsabile del trattamento è l'entità che elabora i dati personali per conto del titolare del trattamento, che, con il GDPR, ove appartenente all'organizzazione di quest'ultimo, si identifica con il mero soggetto autorizzato al trattamento.

Il Titolare del Trattamento è reperibile al seguente indirizzo: presidente@opisiena.it

Il recapito telefonico e l'indirizzo e-mail sono i seguenti: 0577-281160

Autorizzati al trattamento

Sono "*persone autorizzate al trattamento*", coloro che svolgono il trattamento sotto l'autorità diretta del titolare o del responsabile.

Il GDPR non prevede espressamente l'obbligo di nomina scritta dei soggetti autorizzati.

Più dell'atto formale di nomina è fondamentale "l'istruzione" di tali soggetti al rispetto delle norme in materia di protezione dei dati personali.

È opportuno, pertanto, prevedere percorsi formativi adeguati a coloro che sono coinvolti a tale titolo nel trattamento dati.

Nel GDPR gli incaricati corrispondono alle persone autorizzate al trattamento, cioè a coloro che svolgono il trattamento sotto l'autorità diretta del titolare o del responsabile.

Interessato

Interessato: la persona fisica cui si riferiscono i dati personali.

Referente privacy

Le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più o soggetti autorizzati (o designati).

Terzo

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare del trattamento o del responsabile del trattamento.

4 PRINCIPI GENERALI DEGLI ORDINI PROFESSIONALI

Gli Ordini provinciali sono enti di diritto pubblico non economico, istituiti e regolamentati da apposite leggi come Collegi (Legge 29 ottobre 1954, n. 1049, Dlcps 233/46 e Dpr 221/50) e dalla legge 3/2018 come Ordini.

La norma affida agli Ordini (ex Collegi) una finalità esterna e una finalità interna.

La prima è la tutela del cittadino/utente che ha il diritto, sancito dalla Costituzione, di ricevere prestazioni sanitarie da personale qualificato, in possesso di uno specifico titolo abilitante, senza pendenze rilevanti con la giustizia ecc.

La seconda finalità è rivolta agli infermieri iscritti all'Albo, che l'Ordine è tenuto a tutelare nella loro professionalità, esercitando il potere disciplinare, contrastando l'abusivismo, vigilando sul rispetto del Codice deontologico, esercitando il potere tariffario, favorendo la crescita culturale degli iscritti, garantendo l'informazione, offrendo servizi di supporto per un corretto esercizio professionale.

L'organo di governo dell'Ordine è il Consiglio direttivo, che si rinnova ogni quadriennio attraverso una consultazione elettorale di tutti gli iscritti.

Ogni Consiglio distribuisce al proprio interno le cariche di presidente, vicepresidente, segretario e tesoriere.

Il presidente ha la rappresentanza dell'Ordine provinciale ed è membro di diritto del Consiglio nazionale.

L'Albo professionale è uno strumento attraverso il quale l'Autorità giudiziaria e quella amministrativa possono conoscere coloro che esercitano una determinata professione per vigilare sulla loro attività ed anche applicare quelle sanzioni cui possono andare incontro.

I Professionisti Sanitari hanno un diritto assoluto, avendone i requisiti, ad ottenere l'iscrizione nell'Albo.

Il relativo atto ha natura di atto dovuto e senza di esso i professionisti non possono esercitare diritti che conseguono alla professione.

I dati pubblicati, ai sensi dell'art.3 del DPR 7 agosto 2012 n. 137, sono gestiti ed aggiornati dai titolari degli stessi, ovvero i singoli Collegi provinciali che hanno competenza legislativa circa la tenuta, l'aggiornamento degli Albi, e le iscrizioni/cancellazioni. (DLCPS 233/46 e DPR 221/50).

A loro è quindi demandata la competenza a rilasciare apposite certificazioni.

Gli albi territoriali relativi alle singole professioni regolamentate, tenuti dai rispettivi consigli dell'ordine o del collegio territoriale, sono pubblici e recano l'anagrafe di tutti gli iscritti, con l'annotazione dei provvedimenti disciplinari adottati nei loro confronti.

L'insieme degli albi territoriali di ogni professione forma l'albo unico nazionale degli iscritti, tenuto dal consiglio nazionale competente.

I consigli territoriali forniscono senza indugio per via telematica ai consigli nazionali tutte le informazioni rilevanti ai fini dell'aggiornamento dell'albo unico nazionale.

5 OBIETTIVO DEL MODELLO PRIVACY E DATI TRATTATI DA OPI SIENA

L'obiettivo del presente Modello organizzativo è quello dare evidenza delle attività di trattamento dei dati secondo un principio di trasparenza: secondo il GDPR, se il processo di trattamento dei dati è trasparente, diventa anche sicuro (considerando 58, 59, 60).

Gli Ordini hanno l'obiettivo di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, eseguendo le seguenti principali attività:

- la designazione del DPO;
- la comunicazione del DPO all'Autorità Garante per la Protezione dei Dati Personali;
- l'istituzione del Registro dei trattamenti;
- l'esame dei rapporti contrattuali con i responsabili esterni del trattamento e la conseguente adozione eventuale di un contratto per il trattamento dei dati e nomina a responsabile;
- la redazione delle informative per ogni tipologia di dato trattato;
- la verifica dell'adozione delle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato ai trattamenti effettuati, tenendo conto di quelle già adottate, ivi incluse quelle di cui allo schema di regolamento proposto dal Ministero della Giustizia;
- l'adozione di procedure interne per la gestione di eventuali data breach;
- l'avvio di attività interne di formazione e sensibilizzazione GDPR e i suoi impatti sulle attività dell'Ordine.

I dati personali trattati da OPI Siena sono prevalentemente i seguenti:

- **Dati personali relativi alla gestione dei dipendenti, al reperimento ed inserimento di nuovo personale e collaboratori**
- **Dati personali degli iscritti o dei richiedenti iscrizione**
- **Dati personali dei componenti del Consiglio direttivo e di ogni altra figura istituzionale.**

6 POLITICA DI OPI SIENA

L'Ordine delle professioni infermieristiche di SIENA si impegna al trattamento dei dati dell'interessato in modo lecito, corretto e trasparente.

I dati vengono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il loro trattamento non sia incompatibile con tali finalità.

I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

OPI Siena, inoltre, si impegna perché i dati raccolti siano esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

I dati vengono, altresì, conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, trattati in maniera da garantire un'adeguata sicurezza dei dati personali,

compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Gli impegni richiamati nel presente documento di politica sono validi, oltre che per i trattamenti dei dati personali di cui OPI Siena è Titolare, anche per tutti quei trattamenti di cui OPI Siena è nominata Responsabile del trattamento da altri Titolari del trattamento, salvo la presenza di misure più restrittive in materia di protezione dei dati personali contenute nei documenti che regolano i rapporti con il Titolare del trattamento.

La presente Politica e le misure di sicurezza richiamate nel presente documento sono condivise con ogni soggetto terzi con il quale OPI Siena affida l'incarico di Responsabile del trattamento.

6.1 ORGANIGRAMMA

OPI Siena garantisce la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali con la precisa individuazione dei soggetti che ricoprono ruoli attivi nel trattamento.

L'organigramma privacy viene aggiornato in occasione di qualsiasi variazione intervenuta.

Ogni Ordine si qualifica, ai fini privacy, come titolare del trattamento e, pertanto, ogni Ordine territoriale deve ritenersi come un autonomo centro di imputazione degli adempimenti in materia di protezione dei dati personali.

Titolare del trattamento: è l'Ordine che, ai fini privacy, agisce per il tramite del Consiglio, in persona del Presidente e legale rappresentante pro tempore.

Conformemente a quanto previsto dalla normativa l'ente è Titolare del trattamento e in tale ruolo si impegna a:

- adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;
- adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi

almeno il:

- diritto all'accesso, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare, l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi

- identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento;
- diritto alla rettifica, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;
- diritto alla cancellazione, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- diritto all'opposizione, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti.

Al fine di esercitare i diritti sopra descritti, OPI Siena si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

Responsabili del trattamento: il ruolo del responsabile esterno è del tutto diverso da quello di un eventuale responsabile interno: mentre il primo è un'entità – fisica o giuridica – "altra" rispetto al titolare e da questo autonoma, il secondo ne è diretta emanazione e, in merito al trattamento dei dati personali, è una "persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare".

Compiti dei responsabili del trattamento sono quelli di:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge
- predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento, qualora sia necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- nominare i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- controllare le operazioni di trattamento svolte dai soggetti autorizzati sottoposti alla propria responsabilità e la conformità all'ambito di trattamento consentito;
- redigere e aggiornare la lista dei nominativi dei soggetti autorizzati sottoposti alla propria responsabilità e verificarne almeno annualmente l'ambito di trattamento consentito;

- proporre al Titolare del trattamento dei dati la nomina di soggetti per il ruolo di sub-Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore inoltrando al Titolare del trattamento le richieste pervenute nel caso non possano essere evase autonomamente;
- distruggere i dati personali alla fine del trattamento nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare del trattamento;

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento può modificare la propria struttura per conseguire i migliori risultati di protezione variando opportunamente l'articolazione del proprio Sistema di Gestione Privacy.

Soggetti autorizzati: sono tutti i soggetti interni all'organizzazione dell'Ordine, che sono operativamente coinvolti nelle attività di trattamento. Secondo gli articoli 28 e 29 del Regolamento gli incaricati del trattamento, gestiscono i dati personali per conto del titolare che ha fissato finalità e modalità del trattamento (si è provveduto, attraverso la condivisione del presente Modello Organizzativo Privacy in un incontro formativo ad informare e responsabilizzare gli incaricati relativamente al proprio compito).

L'organigramma privacy, descritto nel presente documento, deve ritenersi sicuro in quanto intende garantire la disponibilità, l'integrità e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, attraverso l'attribuzione di specifici incarichi, la certificazione delle fonti di provenienza dei dati e le istruzioni per le persone autorizzate ad effettuare i trattamenti.

I compiti degli autorizzati al trattamento sono di seguito sintetizzati:

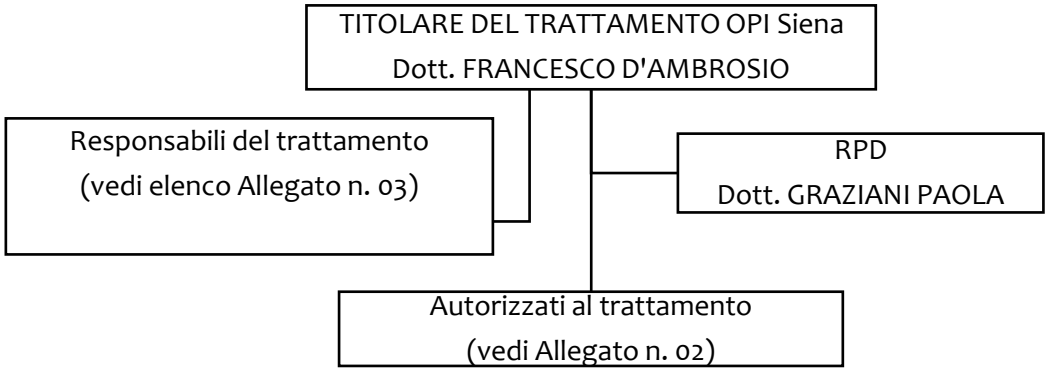
- segnalare al DPO eventuali casi di violazioni dei dati personali, segnalati da parte di terzi o autonomamente individuati;
- segnalare al DPO eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- cooperare in caso di attività di controllo nell'ambito della protezione dei dati personali fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;
- informare il DPO dell'esistenza di un nuovo progetto che impatta sulla protezione dei dati, in applicazione del principio di privacy by design e by default;
- informare il DPO dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornare il registro o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il DPO della presenza di una nuova risorsa che tratta dati personali al fine di valutare necessità di formazione in ambito privacy;
- rispettare le indicazioni impartite da OPI Siena;

- segnalare al DPO eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- avvisare il DPO, se nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti ed eseguire almeno un'analisi dei rischi, in applicazione dei principi di privacy by design e privacy by default;
- informare immediatamente il DPO, qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
- segnalare al DPO, eventuali accessi non autorizzati;
- rilasciare all'interessato l'informativa e acquisire il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento).

Referenti privacy: i compiti del soggetto Referente privacy, autorizzato con apposito atto, sono di seguito sintetizzati:

- individuare le persone da autorizzare al trattamento dei dati e promuoverne l'autorizzazione per area di competenza;
- segnalare al DPO eventuali casi di violazioni dei dati personali, segnalati da parte delle risorse ad esso assegnate o autonomamente individuati;
- segnalare al DPO eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- cooperare in caso di attività di controllo nell'ambito della protezione dei dati personali da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;
- informare il DPO dell'esistenza di un nuovo progetto che impatta sulla protezione dei dati, in applicazione del principio di privacy by design e by default;
- informare il DPO dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornare il registro o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il DPO della presenza di una nuova risorsa che tratta dati personali al fine di valutare necessità di formazione in ambito privacy;
- controllare che le persone autorizzate al trattamento rispettino le indicazioni impartite dall'ente.

DPO: Alla luce degli obblighi previsti in materia di trattamento dei dati personali, il Titolare ha nominato ai sensi dell'art.37 del Regolamento Ue 2016/679 il Data Protection Officer (DPO).



La struttura organizzativa e funzionale di OPI Siena prevede che il trattamento di dati sia effettuato, per le rispettive competenze:

- Dal personale interno secondo l'Allegato 02 "Elenco personale autorizzato";
- Da soggetti esterni nell'ambito della prestazione di specifici servizi secondo l'Allegato 03 "Elenco responsabili esterni del trattamento".

Consiglio Direttivo

Presidente	
Francesco D'Ambrosio	presidente@opisiena.it
Vicepresidente	
Lorenzo Righi	vicepresidente@opisiena.it
Segretario	
Maria Martina Tedesco	segretario@opisiena.it
Tesoriere	
Rodrigo Antonio Lopez Pollan	tesoriere@opisiena.it
Consiglieri	
Stefano Bugnoli	bugnoli.stefano@cert.ordine-opi.it
Alice Cavagnini	cavagnini.alice@cert.ordine-opi.it
Fabrizio Mario Di Salvo	disalvo.fabrizio.mario@cert.ordine-opi.it
Daniela Fabbri	fabbri.daniela@cert.ordine-opi.it
Daniela Ginanneschi	ginanneschi.daniela@cert.ordine-opi.it
Alessia Muratori	muratori.alessia@cert.ordine-opi.it
Angelo Nuzzo	nuzzo.angelo@cert.ordine-opi.it
Carla Raddavero	raddavero.carla@cert.ordine-opi.it
Isemann Christian Ramacciani	christian@pec.criweb.eu
Moris Rosati	rosati.moris@cert.ordine-opi.it
Sara Vanni	vanni.sara@cert.ordine-opi.it

Commissione Albo

Costituita con la legge 3/2018, come previsto dagli art. 2 e 3, i compiti delle Commissioni di Albo sono:

- proporre al Consiglio Direttivo l'iscrizione all'albo del professionista, valutando quindi i titoli di studio;
- assumere la rappresentanza della Professione;
- nominare i rappresentanti della Professione presso commissioni, enti ed organizzazione di carattere istituzionale;
- promuovere e favorire le iniziative intese a facilitare il progresso culturale degli iscritti, anche in riferimento alla formazione universitaria finalizzata all'accesso alla professione;
- difendere la professione, interponendosi nelle controversie fra gli iscritti, o fra un iscritto e persona o ente;
- adottare e dare esecuzione ai provvedimenti disciplinari nei confronti di tutti gli iscritti all'albo e a tutte le altre disposizioni di Ordine disciplinare e sanzionatorio contenute nelle leggi e nei regolamenti in vigore;
- esercitare le funzioni gestionali comprese nell'ambito delle competenze proprie, come individuate dalla legge e dallo statuto;
- dare il proprio concorso alle autorità locali nello studio e nell'attuazione dei provvedimenti che comunque possano interessare la professione.

- **Presidente**
- Giovanna Millozzi: millozzi.giovanna@cert.ordine-opi.it
- **Vicepresidente**
- Maria Giuliano: giuliano.maria@cert.ordine-opi.it
- **Segretario**
- Beatrice Arezzini: arezzini.beatrice@cert.ordine-opi.it
- **Consiglieri**
- Daniele Angelini: angelini.daniele@cert.ordine-opi.it
- Denis Angelo Continanza: continanza.denis@pec.it
- Barbara Pasqualini: zara2018@postecertifica.it
- Roberto Pipitone: pipitone.roberto@cert.ordine-opi.it

Collegio dei Revisori Dei Conti

Per ciascun OPI provinciale e per la Federazione nazionale è eletto un Collegio dei revisori dei conti composto da tre membri effettivi e da un supplente.

Essi durano in carica per il periodo previsto per i Consigli direttivi e per il Comitato centrale.

Le attività dei Collegio dei revisori dei conti sono disciplinate anche dal Regolamento di contabilità approvato dal Ministero della Salute, sia per i Collegi che per la Federazione.

Presidente

Emanuela Farina

Revisori Effettivi

Roberta Melaragni

Adriano Minucci

Revisore Supplente

Elisa Barneschi

7 TRATTAMENTI DEI DATI EFFETTUATI DA OPI SIENA

7.1 Trattamento dati dei dipendenti e collaboratori

I dati sono trattati per la gestione del rapporto di lavoro o di collaborazione.

In questi trattamenti rientrano quelli effettuati:

- per esigenze di verifica dell'idoneità e dell'attitudine a svolgere prestazioni;
- per adempimenti connessi all'adesione a sindacati o ad organizzazioni di carattere sindacale o similari;
- per esigenze derivanti dalle opinioni politiche, credenze religiose e dalle convinzioni filosofiche o da simili orientamenti d'altro genere;
- per adempimenti connessi all'origine etnica, ivi inclusi i benefici previsti dalla legge;
- per gestione della struttura organizzativa, dell'anagrafica del personale e registrazione degli eventi di carriera;
- per adempimenti relativi a riserve di legge e maternità o paternità;
- per rilevazione e gestione delle presenze;
- per esigenze di igiene e sicurezza sul luogo di lavoro;
- per svolgimento di pratiche assicurative, assistenziali o previdenziali, ivi incluse quelle inerenti denunce di infortuni, sinistri e/o indennizzi;
- per garantire la fruizione di particolari esenzioni o permessi lavorativi per il personale dipendente;
- per gestione della formazione;
- per erogazione della retribuzione, dei compensi e di ogni accessorio;
- per mutamenti inerenti al rapporto, tra cui mobilità e trasferimenti;
- per programmazione annuale degli obiettivi e per valutazione del personale;
- per avvio, istruttoria e chiusura di procedimenti disciplinari;
- per gestione di procedimenti amministrativi e giurisdizionali inerenti al rapporto di lavoro o collaborazione, ivi inclusi quelli di natura conciliativa.

I dati trattati in questo caso sono:

- Dati personali
- Dati sensibili e giudiziari aventi ad oggetto: stato di salute del dipendente o collaboratore;
- dati inerenti alla salute di familiari del dipendente o collaboratore;
- origine etnica del dipendente o collaboratore;

- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile del dipendente o collaboratore;
- vita sessuale del dipendente o collaboratore, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- informazioni sul dipendente o collaboratore contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Le modalità di trattamento sono:

- Raccolta presso gli interessati e presso terzi.
- Elaborazione con documenti cartacei e con modalità informatiche.

La base giuridica del trattamento è la seguente:

Normativa legislativa e regolamentare inerente in generale il personale assunto dell'ente pubblico non economico identificato nell'Ordine, tra cui quella in materia di:

- impiego pubblico, ivi inclusa quella disciplinare, di formazione, di occupazione, di maternità e paternità e di mobilità;
- conferimento di incarichi individuali di collaborazione, formazione, ricerca e studio;
- assicurativa, assistenziale, previdenziale e sindacale;
- sicurezza e salute sui luoghi di lavoro;
- documentazione amministrativa, ivi inclusa quella sul relativo accesso;
- anticorruzione, codice di condotta dei dipendenti pubblici e trasparenza;
- amministrazione digitale;
- amministrazione e contabilità degli enti pubblici non economici;
- procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.
- Contratto collettivo nazionale del comparto enti pubblici non economici.
- Contratto individuale di lavoro subordinato, di lavoro parasubordinato o di prestazione d'opera.

Interessati al trattamento:

- Dipendente o collaboratore.
- Familiari del dipendente o collaboratore.

Destinatari dei dati

- Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.
- Organizzazioni sindacali relativamente ai dipendenti iscritti.
- Enti assistenziali, previdenziali e assicurativi e autorità legali di pubblica sicurezza ai fini assistenziali e previdenziali, nonché per rilevazione di eventuali patologie o infortuni sul lavoro.
- Compagnie di assicurazioni su richiesta dell'interessato o qualora sia previsto dal contratto di assicurazione.
- Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive.
- Uffici competenti per il collocamento obbligatorio, relativamente ai dati anagrafici degli assunti appartenenti alle "categorie protette".
- Enti di appartenenza dei lavoratori per definire il trattamento retributivo del dipendente.
- Ministero dell'Economia e Finanze nel caso in cui l'ente svolga funzioni di centro assistenza fiscale.

- Enti competenti in materia di igiene e sicurezza nei luoghi di lavoro.
- Strutture sanitarie competenti per visite fiscali e medico competente.
- Soggetti pubblici e privati ai quali ai sensi delle leggi regionali/provinciali viene affidato il servizio di formazione del personale.
- Autorità giudiziarie.
- Collegi di conciliazione.
- Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge, anche quelle di pubblica sicurezza.

Conservazione dei dati

Per tutti i trattamenti: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

7.2 Dati personali degli iscritti o dei richiedenti iscrizione

I dati di iscrizione all'albo pubblicati, ai sensi dell'art. 3 del DPR 7 agosto 2012 n. 137, sono gestiti ed aggiornati dai titolari degli stessi, ovvero i singoli Ordini provinciali che hanno competenza legislativa circa la tenuta, l'aggiornamento degli Albi, e le iscrizioni/cancellazioni. (DLCPS 233/46 e DPR 221/50).

A loro è quindi demandata la competenza a rilasciare apposite certificazioni.

I dati personali degli iscritti o dei richiedenti l'iscrizione sono:

- Dati fiscali, di identità ed altre informazioni o richieste documentali relative ai requisiti previsti per la prima iscrizione e per il mantenimento dell'iscrizione all'albo quali ad esempio: residenza, cittadinanza, diplomi e crediti relativi a percorsi formativi, pagamento di quote o tasse di iscrizione.;
- Dati relativi a corsi e altri servizi erogati da OPI Siena o da terzi richiesti e/o utilizzati dal richiedente;
- Dati particolari relativi al casellario giudiziario in caso di richiedenti prima iscrizione o, nel caso di soggetti già iscritti, a seguito di procedimenti disciplinari attivati da OPI Siena o in base a richieste degli enti giudiziari o di polizia in relazione a indagine penale, civile o amministrativa.

OPI Siena NON raccoglie nessun dato ai fini di controllo o profilazione dell'interessato.

Finalità del trattamento dei dati

Il principio della trasparenza si concretizza in un obbligo da parte titolare del trattamento di informativa privacy con informazioni concise, facilmente accessibili e di facile comprensione, ma anche con la predisposizione chiara di procedure che diano la possibilità all'interessato di esercitare agevolmente i diritti che gli spettano, come l'accesso ai dati, la loro rettifica e cancellazione e il diritto di opposizione.

Tutto si basa sull'idea di accountability, ossia sul fatto che ogni azione di conformità sia esito di un'analisi del rischio, che abbia un aspetto di sostanza ma anche che sia facilmente dimostrabile e verificabile.

Il presente Modello Organizzativo disciplina l'attuazione di quanto disposto dal Regolamento GDPR n°2016/679 del

Parlamento Europeo e del Consiglio del 27 aprile 2016, dal D.Lgs. 30 giugno 2003 n° 196, Codice in materia di protezione dei dati personali e s.m.i, dal D.Lgs. 10 agosto 2018 n° 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, dal Disciplinare tecnico in materia di misure minime di sicurezza, dai provvedimenti collegati emanati dall'Autorità garante per la protezione dei dati personali.

Per tutto quanto non è dettagliatamente disciplinato nel presente Modello Organizzativo, si rinvia a quanto disposto dal GDPR 2016/679, dal Codice in materia di protezione dei dati personali, D.Lgs. 196/2003 e dal D.Lgs. 101/2018 e provvedimenti collegati.

È sulla base del rispetto del principio di trasparenza che vengono di seguito indicate le finalità ed il presupposto del trattamento a cui sono destinati i dati personali.

a) TENUTA DELL'ALBO PROFESSIONALE

I dati personali degli iscritti o richiedenti iscrizione potranno essere trattati per l'adempimento ad obblighi previsti da leggi, regolamenti o da altre norme, da provvedimenti dell'autorità giudiziaria, ovvero in base ad obblighi contabili, retributivi, assistenziali o fiscali (Art. 6 c. 1 lett. c, lett. e RGPD). La principale attività di OPI Siena è la tenuta dell'Albo professionale, da ciò ne consegue, ai sensi dell'art. 9 del DLCPS 233/46 e art. 4 del DPR 221/50 e norme successive, l'esigenza di acquisire e trattare i dati personali degli iscritti, di darne la pubblicità derivante dalla natura di pubblico registro dell'Albo, attuare la vigilanza sul rispetto del codice deontologico, curare la formazione permanente e la partecipazione degli iscritti alla formazione ed al funzionamento degli organi, fornire agli iscritti i servizi previsti dalle norme di legge, dallo statuto e in esecuzione di delibere degli organi dell'Ente.

b) ATTIVITA' ISTITUZIONALI

Attività istituzionali sono anche l'informazione agli iscritti relativa alle attività dell'Ente, alla loro partecipazione alla formazione ed al funzionamento degli organi dell'Ordine, a norme, circolari e documentazione relativa alle professioni infermieristiche e all'ambito sanitario di interesse per gli associati, l'informazione e la promozione in relazione ad attività formative, servizi o nuove iniziative rientranti tra le finalità dell'Ente e da questo organizzate o patrocinate. L'interessato al trattamento, qualora intenda iscriversi o mantenere l'iscrizione all'Albo, accetta di conferire i dati personali necessari a tali finalità ed il relativo trattamento non necessita del consenso dell'interessato. Sarà invece cura dell'interessato collaborare per mantenere i dati corretti e aggiornati, segnalando tempestivamente errori o modifiche che dovessero interessare i propri dati. Per tali attività verranno utilizzati i dati ed i canali di comunicazione già acquisiti dall'Ente nei rapporti istituzionali con l'interessato, attraverso lettere, telefono, posta elettronica o altri strumenti di comunicazione.

Nel caso di trattamenti connessi all'esecuzione di attività formative, di consulenza o altri servizi o altri rapporti di natura contrattuale che l'interessato ha richiesto o ai quali ha aderito (Art. 6 c. 1 lett. b RGPD), il conferimento dei dati personali necessari a tali finalità non è obbligatorio, ma il rifiuto di fornirli può comportare, in relazione al rapporto tra il dato e l'adempimento richiesto, l'impossibilità dell'Ente di eseguire l'attività stessa o parte di essa o di adempiere a richieste specifiche dell'interessato preliminari all'esecuzione della richiesta o alla conclusione di un contratto. Qualora tali dati vengano forniti, il consenso al loro trattamento si ritiene implicito nella richiesta dell'interessato.

c) ALTRE ATTIVITA'

Altre informazioni e comunicazioni non istituzionali (Art. 6 c. 1 lett. a RGPD). Rientrano in questa categoria: l'informazione e la promozione relativa a iniziative, corsi, convegni e altre attività formative o culturali organizzate da soggetti terzi e/o

promossa da OPI Siena, l'informazione su concorsi, selezioni e altre opportunità di lavoro professionale o a titolo di volontariato pervenute o segnalate a OPI Siena, la diffusione dei propri dati personali comuni, previa richiesta, tramite pubblicazione sul sito istituzionale OPI Siena. Per tali attività verranno utilizzati i dati ed i canali di comunicazione già acquisiti dall'Ente nei rapporti istituzionali con l'interessato, attraverso lettere, telefono, posta elettronica o altri strumenti di comunicazione. Il conferimento dei dati personali necessari a tali finalità non è obbligatorio e il loro trattamento richiede uno specifico consenso. Qualora l'interessato voglia opporsi al trattamento dei propri dati in relazione a queste finalità, può farlo in qualunque momento, mediante semplice richiesta scritta o via e-mail inviata al Responsabile Protezione Dati (RPD) incaricato dott.ssa Paola Graziani e-mail: paograz.gp@pec.libero.it presso l'Ordine delle Professioni infermieristiche di Siena– Viale Europa 31, Cap. 53100 Siena (SI), specificando il tipo di trattamento ed il canale attraverso il quale non desideri più essere contattato. Tale revoca non pregiudica la liceità del trattamento basato sul consenso precedentemente prestato.

d) COOKIE POLICY

OPI Siena utilizza per il proprio sito istituzionale unicamente cookie c.d. "tecnici": si tratta di cookie che servono a effettuare la navigazione o fornire un servizio richiesto dall'utente. NON si impiega nessun cookie ai fini di controllo o profilazione dell'interessato. Per ulteriori dettagli si rimanda alla cookie policy presente sul sito https://www.opisiena.it/.

Tempi di conservazione dei dati personali

I dati personali vengono conservati solo per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per qualsiasi altra legittima finalità collegata.

Se i dati personali sono trattati per due o più finalità, essi verranno conservati fino a che non sarà cessata la finalità con il termine di conservazione previsto più lungo.

I dati personali che non siano più necessari o per i quali non vi sia più un presupposto giuridico per la relativa conservazione vengono anonimizzati irreversibilmente (e in tal modo potranno essere conservati) o distrutti in modo sicuro.

Salvo che la legge non imponga specifiche esigenze di conservazione, i dati personali sono conservati per l'intera durata dell'iscrizione e per un termine ulteriore pari a 10 anni e sei mesi dall'estinzione del rapporto, in considerazione dei termini di prescrizione di diritti od obblighi in relazione ai quali l'Ente potrebbe avere necessità di difendersi o adempiere o delle esigenze di conservazione imposte dalla normativa.

Con riferimento ai dati funzionali all'instaurazione del rapporto, laddove non perfezionato, gli stessi saranno conservati per un termina massimo di 12 mesi, al fine di mettere in condizione OPI Siena di poter rispondere a specifiche richieste dell'interessato.

I dati giudiziari degli interessati vengono conservati per un periodo di 6 mesi, dopo il completamento delle procedure di iscrizione o per le quali vengono raccolti e trattati e vengono poi distrutti in modo sicuro.

Luoghi di conservazione dei dati personali

Tutti i dati personali sono conservati su server protetti o documenti cartacei idoneamente archiviati o su altri supporti elettronici (server, cloud, ecc.) di fornitori di servizi di OPI Siena che sono stati specificamente autorizzati al trattamento in base agli standard e alle policy di sicurezza o standard equivalenti di OPI Siena.

Il dettaglio delle modalità tecniche e organizzative per il trattamento e le relative misure di sicurezza è disponibile, a richiesta, presso OPI Siena, Titolare del trattamento.

Accesso ai dati personali

Ai dati personali possono avere accesso i consiglieri di amministrazione ed i dipendenti debitamente autorizzati, nonché i fornitori esterni nominati, se necessario, responsabili del trattamento, che forniscono supporto a OPI Siena per l'erogazione dei servizi dell'ordine.

L'elenco di detti enti, società o imprese è allegato al presente documento (Allegato n. 03) disponibile presso la sede dell'Ente stesso o può essere richiesto mediante semplice richiesta scritta o via e-mail inviata al Responsabile Protezione Dati (RPD) incaricato dott.ssa Paola Graziani presso l'Ordine delle Professioni infermieristiche di Siena.

In relazione alla normativa vigente, i medesimi dati sono messi a disposizione del pubblico mediante accesso regolato e comunicati alle altre autorità ed amministrazioni pubbliche con le quali l'Ordine si rapporta per esigenze di pubblico interesse, in base alle norme che regolano le professioni infermieristiche.

Solo su specifica richiesta dell'interessato, una parte limitata dei propri dati comuni potrà essere diffusa attraverso l'inserimento nell'elenco dei professionisti pubblicato sul sito istituzionale OPI Siena.

Con la diffusione dei propri dati personali, OPI Siena non avrà più alcun controllo sui dati diffusi e tali dati potrebbero essere utilizzati da soggetti terzi, anche in paesi Extra UE, anche per finalità diverse da quelle previste con la pubblicazione.

Il titolare non trasferisce i dati personali in Paesi nei quali non è applicato il RGPD (paesi extra UE) salvo specifiche indicazioni contrarie per le quali verrà preventivamente informato e, se necessario, acquisito il consenso.

Diritti dell'interessato

Come previsto dal RGPD, l'interessato ha il diritto di chiedere all'Ente:

- l'accesso ai Suoi dati personali;
- la copia dei dati personali che ha fornito (c.d. portabilità);
- la rettifica dei dati in possesso di OPI Siena;
- la cancellazione di qualsiasi dato per il quale non si abbia più alcun presupposto giuridico per il trattamento;
- l'opposizione al trattamento ove previsto dalla normativa applicabile;
- la revoca del consenso, nel caso in cui il trattamento sia fondato sul consenso;
- la limitazione del modo in cui vengono trattati i Suoi dati personali, nei limiti previsti dalla normativa a tutela.

Tali diritti possono essere esercitati mediante richiesta scritta inviata al Responsabile Protezione Dati (RPD) incaricato dott.ssa Graziani Paola presso l'Ordine delle Professioni infermieristiche di Siena– Viale Europa 31, Cap. 53100 SIENA (SI) o a mezzo e-mail: paograz.gp@pec.libero.it.

Tali diritti soggiacciono ad alcune eccezioni finalizzate alla salvaguardia dell'interesse pubblico (ad esempio, il non esercizio della professione infermieristica ai fini della cancellazione dall'Albo) e degli altri interessi pubblici e dell'Ente.

Nel caso in cui l'interessato esercitasse uno qualsiasi dei summenzionati diritti, sarà onere di OPI Siena verificare che sia legittimato ad esercitarlo, dando riscontro, di regola, entro un mese.

Reclami

In relazione alle segnalazioni o richieste circa il trattamento dei dati OPI Siena fa ogni sforzo per rispondere alle sue preoccupazioni dell'interessato.

Tuttavia, nel caso non avesse riscontro l'interessato può inoltrare i propri reclami o le proprie segnalazioni al Garante per la protezione dei dati personali – Piazza di Monte Citorio n. 121 – 00186 ROMA.

8 DATI RIEPILOGATIVI DI TRATTAMENTO DEGLI ISCRITTI O RICHIEDENTI ISCRIZIONE ALL'ALBO

8.1 Denominazione del trattamento: abilitazione alla professione e tenuta e gestione dell'albo.

Descrizione e scopo del trattamento: i dati sono trattati al fine di consentire agli interessati di iscriversi all'Albo.

I dati sono, inoltre, trattati per la gestione e la tenuta dell'Albo.

In questi trattamenti rientrano quelli effettuati per:

- l'acquisizione e verifica della domanda di iscrizione, di cancellazione o di modifica dei dati;
- l'iscrizione all'Albo o all'Elenco speciale;
- la verifica della sussistenza dei presupposti per la permanenza nell'Albo;
- la cancellazione d'ufficio o la radiazione dall'Albo;
- per l'annotazione di provvedimenti disciplinari, ivi inclusa la sospensione dall'esercizio della professione;
- lo svolgimento di attività di vigilanza, di controllo e di monitoraggio connesse alla gestione e alla tenuta relative all'Albo, oltre che all'abilitazione professionale.

Natura di dati trattati

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'iscritto (ivi incluse patologie attuali e pregresse);
- origine etnica dell'iscritto;
- vita sessuale dell'iscritto, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- informazioni sull'iscritto contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Modalità del trattamento

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

Base giuridica del trattamento

Normativa legislativa e regolamentare in materia di riconoscimento di titoli di studio per l'accesso alla professione.

Normativa legislativa e regolamentare inerente all'istituzione dell'Albo.

Normativa legislativa e regolamentare per la tutela del titolo e della professione, ivi inclusa quella inerente all'esercizio abusivo.

Normativa legislativa e regolamentare per la tenuta e la gestione dell'Albo, a seguito di iscrizioni, modifiche di informazioni, cancellazioni e sanzioni disciplinari.

Normativa legislativa e regolamentare in materia di provvedimenti disciplinari da annotare nell'Albo.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Normativa legislativa e regolamentare in materia di previdenza obbligatoria per gli iscritti all'Albo e all'Elenco speciale.

Domanda di iscrizione all'Albo o all'Elenco speciale e successive domande per modifica di dati o cancellazione.

Interessati al trattamento

Iscritti all'Albo

Destinatari dei dati

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Enti previdenziali di iscrizione dell'interessato.

Uffici giudiziari competenti per provvedimenti coinvolgenti l'interessato.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Compagnie di assicurazioni ove richiesto o previsto.

Enti pubblici e privati dai quali l'interessato abbia ricevuto incarichi professionali.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge inerenti agli iscritti all'Albo.

Conservazione dei dati

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi annualmente o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati, a meno che non sia diversamente previsto da disposizioni inderogabili di legge, ivi incluse quelle in materia di documentazione avente rilevanza storica.

8.2 Procedimenti amministrativi e disciplinari coinvolgenti iscritti

Descrizione e scopo del trattamento

I dati sono trattati al fine di avviare, istruire e chiudere procedimenti di natura amministrativa e disciplinare nei confronti di iscritti all'Albo.

In questi trattamenti rientrano quelli effettuati:

- per l'avvio e l'istruttoria di procedimenti relativi alla liquidazione degli onorari;
- per la riscossione di contributi, diritti, tasse, tributi e altri oneri nei confronti degli iscritti;
- per l'avvio e l'istruttoria di altri procedimenti amministrativi su istanza di parte o d'ufficio;
- per le comunicazioni di tutti i provvedimenti amministrativi;
- per l'avvio e l'istruttoria di procedimenti disciplinari su segnalazione o d'ufficio;
- per le comunicazioni di sanzioni disciplinari;
- per lo svolgimento di attività di vigilanza, di controllo e di monitoraggio sull'esercizio dell'attività professionale.

Natura di dati trattati

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'iscritto (ivi incluse patologie attuali e pregresse);
- dati inerenti alla salute dei familiari dell'iscritto;

- vita sessuale dell'iscritto, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'iscritto;
- informazioni sull'iscritto contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Modalità del trattamento

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

Base giuridica del trattamento

Normativa legislativa e regolamentare inerente ai procedimenti disciplinari.

Normativa legislativa e regolamentare inerente alla liquidazione degli onorari.

Normativa legislativa e regolamentare in materia di amministrazione e contabilità degli enti pubblici non economici, ivi inclusa quella relativa ai loro bilanci.

Normativa legislativa e regolamentare inerente alla riscossione di contributi, diritti, tasse, tributi e altri oneri dovuti dagli iscritti. Normativa legislativa e regolamentare per la tutela del titolo e della professione, ivi inclusa quella inerente all'esercizio abusivo. Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso. Normativa legislativa e regolamentare in materia di amministrazione digitale. Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Normativa legislativa e regolamentare in materia di previdenza obbligatoria per gli iscritti all'Albo e all'Elenco speciale. Normativa legislativa e regolamentare in materia di formazione professionale continua.

Codice deontologico.

Interessati al trattamento

Iscritto all'Albo.

Destinatari dei dati

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Enti previdenziali di iscrizione dell'interessato.

Uffici giudiziari competenti per provvedimenti coinvolgenti l'interessato.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Enti pubblici e privati dai quali l'interessato abbia ricevuto incarichi professionali.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge inerenti agli iscritti all'Albo e all'Elenco speciale.

Conservazione dei dati

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ad anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

8.3 Elezione e nomina degli organi e degli organismi.

Descrizione e scopo del trattamento

I dati sono trattati al fine dell'elezione o della nomina di iscritti all'Albo in organi ed organismi degli Ordini (ivi incluse commissioni e simili).

In questi trattamenti rientrano quelli effettuati:

- per l'indizione e l'organizzazione delle elezioni dei consigli degli Ordini;
- per la nomina del seggio elettorale ai fini delle elezioni dei consigli degli Ordini;
- per le candidature a consiglieri degli Ordini;
- per le operazioni di voto nelle elezioni dei consigli degli Ordini;
- per la proclamazione degli eletti nei consigli degli Ordini;
- per ogni altra operazione necessaria per le elezioni dei consigli degli Ordini;
- per l'avvio, l'istruttoria e la definizione dei procedimenti di nomina di componenti di organi non elettivi ed organismi degli Ordini (ivi incluse commissioni e simili);
- per ogni altra operazione necessaria per la nomina di componenti di organi non elettivi ed organismi degli Ordini (ivi incluse commissioni e simili);
- per la verifica di ipotesi di conflitti di interessi, incandidabilità, incompatibilità ed ineleggibilità inerenti agli organi o organismi degli Ordini (ivi incluse commissioni e simili), nonché per la verifica dei requisiti necessari.

Natura di dati trattati

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Modalità del trattamento

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

Base giuridica del trattamento

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini provinciali.

Normativa legislativa e regolamentare in materia di elezioni del Consiglio Nazionale e degli Ordini provinciali.

Normativa legislativa e regolamentare in materia di nomina di organi ed organismi del Consiglio Nazionale e degli Ordini provinciali.

Normativa legislativa e regolamentare per la tenuta dell'Albo.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Normativa legislativa e regolamentare in materia di formazione professionale continua.

Interessati al trattamento

Iscritti all'Albo.

Destinatari dei dati

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Enti previdenziali di iscrizione dell'interessato.

Uffici giudiziari competenti per provvedimenti coinvolgenti l'interessato.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Compagnie di assicurazioni ove richiesto o previsto.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge inerenti agli iscritti all'Albo.

Conservazione dei dati

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ogni anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

8.4 Attività di formazione degli iscritti all'albo

Descrizione e scopo del trattamento

I dati sono trattati al fine della gestione delle attività di iscrizione ed erogazione dei corsi di formazione obbligatoria e facoltativa per iscritti all'Albo.

In questi trattamenti rientrano quelli effettuati:

- per l'iscrizione ai corsi;
- per l'organizzazione dei corsi;
- per l'erogazione della formazione;
- per le attività di valutazione all'esito dei corsi;
- per le attività di controllo, monitoraggio e vigilanza sui corsi erogati e sulla effettiva partecipazione da parte degli iscritti;
- per l'autorizzazione a soggetti terzi ad erogare la formazione;
- per l'esenzione dalle attività formative;
- per controlli sulle autocertificazioni e sulla documentazione prodotta a fini formativi.

Natura di dati trattati

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- stato di salute dei familiari dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Modalità del trattamento

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

Base giuridica del trattamento

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini provinciali.

Normativa legislativa e regolamentare in materia di formazione continua.

Normativa legislativa e regolamentare per la tenuta dell'Albo

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Interessati al trattamento

Iscritto all'Albo o all'Elenco speciale.

Persone fisiche eroganti formazione.

Destinatari dei dati

Organi ed organismi del sistema ordinistico, ivi inclusi i Consigli di disciplina, per i provvedimenti di competenza nei confronti dell'interessato.

Associazioni di Ordini e Ordini di altre professioni presso i quali l'interessato svolga determinate funzioni.

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Enti pubblici e privati eroganti la formazione.

Ministero della Giustizia per pareri sugli enti formatori.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge con riferimento all'erogazione ed alla ricezione di attività formative.

Conservazione dei dati

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ogni anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

8.5 Stipula ed esecuzione di contratti con prestatori di beni, lavori e servizi.

Descrizione e scopo del trattamento

I dati sono trattati al fine di consentire agli interessati di accedere agli affidamenti di prestazioni di beni, lavori e servizi, nonché di eseguire i medesimi, a favore degli Ordini.

In questi trattamenti rientrano quelli effettuati:

- per l'acquisizione delle domande di partecipazione alla procedura per l'affidamento delle prestazioni;
- per la verifica dei requisiti necessari per eseguire le prestazioni;
- per la stipula del contratto avente ad oggetto l'erogazione delle prestazioni;
- per l'esecuzione del contratto, ivi inclusi gli obblighi di pagamento;
- per la gestione di ogni stato patologico del contratto, ivi inclusa la risoluzione;
- per gestione di procedimenti amministrativi e giurisdizionali inerenti al contratto, ivi inclusi quelli per accordi bonari e transazioni.

Natura di dati trattati

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- origine etnica dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- vita sessuale dell'interessato, con riferimento ad una eventuale rettificazione di attribuzione di sesso;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Modalità del trattamento

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

Base giuridica del trattamento

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini provinciali.

Normativa legislativa e regolamentare in materia di contratti pubblici.

Normativa legislativa e regolamentare in materia di documentazione amministrativa.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia assistenziale e previdenziale.

Normativa legislativa e regolamentare in materia di sicurezza e salute sui luoghi di lavoro.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di amministrazione e contabilità degli enti pubblici non economici.

Normativa legislativa e regolamentare in materia di procedimenti, giudiziali e stragiudiziali, di natura amministrativa, civile, contabile, penale e tributaria.

Contratto di prestazione di beni, lavori o servizi.

Interessati al trattamento

Prestatori di beni, lavori e servizi se persone fisiche.

Destinatari dei dati

Amministrazioni in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Enti assistenziali, previdenziali e assicurativi.

Autorità legali di pubblica sicurezza ai fini assistenziali e previdenziali.

Compagnie di assicurazioni dei prestatori.

Enti competenti in materia di igiene e sicurezza nei luoghi di lavoro.

Autorità giudiziarie.

Ogni altra Autorità per la verifica della sussistenza di requisiti contrattuali o di legge nei confronti dei prestatori di beni, lavori o servizi.

Conservazione dei dati

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ogni anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

8.6 Consulenza amministrativo-contabile e legale. contenzioso giudiziale e stragiudiziale

Descrizione e scopo del trattamento

I dati sono trattati al fine di fornire ai consulenti elementi necessari all'espletamento delle consulenze affidate.

In questi trattamenti rientrano quelli effettuati:

- per fornire ai consulenti informazioni necessarie, anche ai fini istruttori o di accertamento, per lo svolgimento delle funzioni istituzionali e per la tutela degli Ordini;
- per fornire ai difensori legali elementi necessari per la tutela degli interessi di difesa e di azione degli Ordini, in sede giudiziale e stragiudiziale, ovvero per istruire la relativa pratica ovvero per la gestione di contenziosi in corso;
- per fornire alle autorità pubbliche competenti per legge, ivi inclusa quella giudiziaria, dati in possesso degli Ordini, anche in caso di richiesta o ordine delle dette autorità.

Natura di dati trattati

Dati personali.

Dati sensibili e giudiziari aventi ad oggetto:

- stato di salute dell'interessato;
- dati inerenti alla salute di familiari dell'interessato;
- origine etnica dell'interessato;
- convinzioni politiche e sindacali, religiose, filosofiche e di altro genere equiparabile dell'interessato;
- vita sessuale dell'interessato;
- informazioni sull'interessato contenute nel casellario giudiziale e nel certificato dei carichi pendenti.

Modalità del trattamento

Raccolta presso gli interessati e presso terzi.

Elaborazione con documenti cartacei e con modalità informatiche.

Base giuridica del trattamento

Normativa legislativa e regolamentare istitutiva del Consiglio Nazionale e degli Ordini Provinciali.

Normativa legislativa e regolamentare in materia di contratti pubblici.

Normativa legislativa e regolamentare in materia di incarichi individuali di collaborazione, consulenza, formazione, ricerca e studio.

Normativa legislativa e regolamentare in materia di documentazione amministrativa, ivi inclusa quella sul relativo accesso.

Normativa legislativa e regolamentare in materia anticorruzione e trasparenza.

Normativa legislativa e regolamentare in materia assistenziale, previdenziale e sindacale.

Normativa legislativa e regolamentare in materia di sicurezza e salute sui luoghi di lavoro.

Normativa legislativa e regolamentare in materia di formazione, obbligatoria o facoltativa, dei professionisti iscritti all'Albo o all'Elenco e dei lavoratori.

Normativa legislativa e regolamentare in materia di amministrazione digitale.

Normativa legislativa e regolamentare in materia di esercizio della professione, ivi inclusa quella relativa all'abilitazione all'esercizio, all'esercizio abusivo e all'interdizione dall'esercizio della professione.

Normativa legislativa e regolamentare in materia di gestione e tenuta dell'Albo e dell'Elenco speciale.

Normativa legislativa e regolamentare in materia di riconoscimento dei titoli di studio per l'accesso alla professione.

Normativa legislativa e regolamentare in materia di amministrazione e contabilità degli enti pubblici non economici.

Normativa legislativa e regolamentare in materia di elezioni e nomine in e da parte di organi ed organismi degli Ordini, anche ai fini del loro commissariamento a seguito di scioglimento.

Normativa legislativa e regolamentare in materia di iscrizione all'Albo o all'Elenco e di ogni connessa modifica.

Normativa legislativa e regolamentare in materia di processi e connessi procedimenti amministrativi, civili, contabili, penali e tributari.

Contratti di prestazione di beni, lavori e servizi.

Contratti di lavoro subordinato, anche collettivi, di lavoro parasubordinato e di collaborazione.

Contratti di prestazioni d'opera professionale, ivi inclusi quelli determinanti il conferimento di mandati alle liti.

Interessati al trattamento

Iscritti all'Albo.

Dipendenti e collaboratori.

Prestatori di beni, lavori e servizi se persone fisiche.

Destinatari dei dati

Avvocatura distrettuale e generale dello Stato, ai fini della gestione del contenzioso giurisdizionale.

Autorità giurisdizionali di qualsiasi ordine e funzione, arbitri, amministrazioni interessate o contro interessate nei vari contenziosi.

Organi di polizia giudiziaria.

Uffici del lavoro ai fini di tentativi di conciliazione.

Autorità e uffici contabili, tributari e fiscali.

Organi consultivi per finalità normative o similari.

Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte quando dovuto.

Compagnie di assicurazione ove richiesto o previsto.

Altre parti, pubbliche o private, coinvolte nel contenzioso, quando dovuto.

Conservazione dei dati

Per tutti i trattamenti, salvi quelli di seguito indicati: 10 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Per i dati trattati ai fini di pagamenti da effettuarsi periodicamente ogni anno o in termini più brevi: 5 anni decorrenti dalla data di cessazione del rapporto da cui deriva il singolo trattamento dei dati.

Al termine del periodo di conservazione i dati verranno cancellati o anonimizzati.

9 RIFERIMENTI NORMATIVI

- ✓ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE)
- ✓ Decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali"
- ✓ Decreto legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).
- ✓ Provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali che, in relazione ai trattamenti effettuati, il titolare è tenuto ad applicare.

10 MISURE DI SICUREZZA

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Queste comprendono un sistema di autenticazione per assicurare che la persona che accede al sistema nelle sue diverse articolazioni sia identificata con certezza, basato su codice identificativo e password individuale segreta, nonché un sistema di autorizzazione che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).

Ad eccezione degli Amministratori di Sistema definiti e nominati secondo le disposizioni del Modello Organizzativo Privacy, nessun dipendente dell'Ordine professionale è Amministratore di Sistema della propria macchina e tutti gli utenti che dispongono di una postazione informatica sono censiti.

Per ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico sono previste una serie di attività, in particolare al momento dell'assunzione o della dimissione delle risorse umane con la procedura di allestimento o dismissione dell'utenza personale.
Sempre al fine di controllo si procede a verificare con cadenza semestrale che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.
Tutti i dispositivi dell'ente concessi in dotazione ai dipendenti vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.
Tutti i dipendenti dell'ente sono pertanto tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne affinché venga assicurata la continuità dei servizi erogati e la conservazione dei documenti di lavoro.

10.1 Misure fisiche

Il titolare del trattamento ha realizzato un adeguato livello di protezione adottando assieme misure organizzative e fisiche, dotandosi di sistemi antintrusione (ad esempio sistemi di allarme, inferriate alle finestre accessibili per posizione, serrande metalliche, presidio da parte del personale dipendente o di soggetti esterni abilitati ecc.).
Le porte di accesso ai locali così come gli arredi dove sono custoditi dati personali sono di buona consistenza.
Ogni posto di lavoro ove opera un incaricato al trattamento dati è dotato di contenitori (cassetto, armadio) con serratura efficiente e sicura.
I dati personali raccolti sono conservati in contenitori adeguati (schedari, armadi) dotati di protezione all'accesso efficiente e sicura.

- Sono indicate, quando necessario, tramite apposita segnaletica, le aree e le modalità di accesso per la clientela (negli uffici, ove possibile, è stata delimitata l'area di accesso al pubblico; in alternativa sono state adottate misure organizzative) ed i locali interdetti al pubblico

Le specifiche misure di protezione sono descritte all'interno delle nomine degli autorizzati al trattamento.

10.2 Misure informatiche

OPI Siena ha definito le modalità del salvataggio dei dati (backup) attraverso una Procedura operativa di backup presente *nell'Allegato A* del presente Modello Organizzativo.
Il titolare del trattamento ha definito le modalità di gestione (attribuzione, cambio, revoca) delle credenziali di autenticazione e dei profili di autorizzazione associati agli autorizzati al trattamento definiti dalla procedura descritta *nell'Allegato B* del presente Modello Organizzativo.
Il titolare del trattamento ha definito le modalità di gestione di idonei strumenti elettronici a protezione dei dati personali contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615-quinquies del codice penale, attraverso la Procedura operativa di gestione dei sistemi di sicurezza (HW e SW) presente *nell'Allegato C* del presente Modello Organizzativo.
Il titolare dispone l'effettuazione dei controlli sugli strumenti elettronici messi a disposizione del personale esclusivamente per:

- Affrontare un evento dannoso o una situazione di pericolo per il sistema informatico che si manifestino nonostante l'adozione di preventivi accorgimenti tecnici;

- Risolvere guasti e malfunzionamenti che riguardano il sistema informatico o singole componenti dello stesso;
- Risolvere situazioni dipendenti da utilizzi non appropriati della rete Internet o della Posta elettronica.

I controlli verranno eseguiti evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori e dei soggetti esterni che ricevano o inviino comunicazioni elettroniche di natura personale e privata, rispettando i principi di pertinenza e non eccedenza e saranno effettuati in modo graduale:

- Basandosi inizialmente, se possibile, su dati aggregati (anonimi) riguardanti l'intera struttura organizzativa o sue aree;
- Avvisando preventivamente il personale dipendente;
- Escludendo controlli ingiustificati e indiscriminati.

Quando utilizzati, il titolare del trattamento dispone la custodia dei supporti rimovibili contenenti dati personali individuando contenitori con idonee caratteristiche di sicurezza.

Il titolare del trattamento dispone e verifica la cancellazione di tutti i dati personali dagli strumenti informatici non più utilizzati o utilizzati in attività diverse da quelle amministrative.

La cancellazione dei supporti prevede il ricorso a procedure, quali:

- Cancellazione sicura delle informazioni, ottenibile con programmi informatici.
- Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF).

Il titolare del trattamento dispone e verifica la distruzione di supporti rimovibili contenenti dati personali non più utilizzati.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a seconda del loro tipo, quali:

- Sistemi di punzonatura o deformazione meccanica.
- Distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd).
- Demagnetizzazione ad alta intensità.

Il titolare, nel caso si dovessero verificare eventi che provochino la distruzione o il danneggiamento dei dati personali contenuti nelle banche dati del sistema informatico, provvederà, senza ritardo, a ripristinare la funzionalità delle banche dati utilizzando le copie di backup.

Il ripristino della disponibilità dei dati andati perduti a causa di eventi di diversa natura consiste di norma:

- Nella re-installazione del software di base, dei programmi, di tutti i file di dati;
- Nella sostituzione di componenti hardware che hanno provocato l'interruzione dei trattamenti.

I tempi per il ripristino della funzionalità del sistema informatico sono contenuti nel limite dei sette giorni.

La re-installazione del software di base, dei programmi e dei file di dati residenti nei PC, la sostituzione di componenti hardware, così come la cancellazione e la distruzione dei supporti saranno disposte dal titolare del trattamento e realizzate anche attraverso soggetti esterni specializzati (manutentore occasionale).

Il titolare del trattamento quando si avvarrà di soggetti esterni per la fornitura di prodotti o servizi finalizzati alla realizzazione di misure minime di sicurezza, si farà consegnare dal soggetto medesimo una descrizione scritta dell'intervento che ne attesti la conformità.

10.3 Misure organizzative

Il titolare del trattamento ha adottato un sistema di autorizzazione in cui i profili degli autorizzati al trattamento dati sono configurati, nel caso di trattamento con strumenti elettronici, e individuati prima dell'inizio del trattamento.

Il titolare del trattamento:

a) Gestisce il sistema di autorizzazione;
b) Forma un elenco degli autorizzati al trattamento, con e senza l'ausilio di strumenti elettronici, con i relativi profili di autorizzazione individuali o per classi omogenee e verifica e integra l'elenco con cadenza annuale;
c) Impartisce istruzioni agli autorizzati finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
d) Impartisce istruzioni agli autorizzati per la distruzione sicura di supporti cartacei contenenti dati personali, riferiti agli interessati, non necessari alle operazioni di trattamento;
e) Affida formalmente, tramite verbali di consegna, agli autorizzati le chiavi di accesso ai locali dove avviene il trattamento di dati personali e impartisce istruzioni sulla corretta gestione delle chiavi dei locali e dei contenitori (schedari, armadi) dove sono conservati i dati personali;
f) Impartisce istruzioni agli autorizzati necessarie ad assicurare la segretezza della componente riservata della credenziale di autenticazione;
g) Impartisce istruzioni agli autorizzati sul corretto utilizzo della rete internet, della posta elettronica e degli strumenti informatici affidati per l'esercizio dell'attività lavorativa, comprese le misure adottate dal titolare per impedire accessi non consentiti a siti web illegali o controversi da parte dei lavoratori, le regole di gestione della posta elettronica e la metodologia adottata per effettuare controlli "graduali" nel caso dovessero sopraggiungere problemi al sistema informatico imputabili all'utilizzo scorretto degli strumenti da parte dei dipendenti;
h) Definisce un elenco dei responsabili (esterni) del trattamento e verifica e integra l'elenco con cadenza annuale.

Il titolare del trattamento consegna in forma scritta la nomina formale agli autorizzati e le istruzioni di cui alle lettere del presente paragrafo e realizza una specifica attività formativa sui temi di cui si tratta; le attività formative sono state registrate.

10.4 Misure logiche

- La Definizione dei profili standard da assegnare agli utenti, con le autorizzazioni necessarie all'espletamento delle rispettive mansioni (definite per ruoli e competenze), avviene alla luce delle effettive esigenze operative. A tal scopo viene limitato l'accesso logico a reti, sistemi e basi dati;
- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da User-ID e password;
- sono adottate delle indicazioni per la gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura richiesta nel caso di trattamenti dei dati effettuati con strumenti elettronici;
- sono previsti sistemi per la periodica validazione e il censimento delle utenze e delle abilitazioni;
- sono adottate tecniche e metodologie per la verifica continua dell'utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato, al fine di garantire un pronto intervento in caso di attività anomale;
- sono previsti presidi rafforzati per l'accesso da remoto, in particolare nei confronti di utenti
- appartenenti a soggetti terzi;
- è prevista la revisione periodica delle misure di sicurezza, anche attraverso esercizi di penetration test, al fine di

prevenire violazioni dei dati personali (Data Breach);

- sono organizzate sessioni di formazione dei dipendenti, nonché regolamenti e altre forme di documentazione interna, al fine di rendere gli stessi edotti dei rischi in materia di sicurezza delle informazioni e di protezione dei dati personali;
- sono previsti periodici controlli al fine di verificare l'adeguatezza, l'affidabilità complessiva e la tutela del sistema informativo.

10.5 Misure specifiche di dati personali idonei a rivelare lo stato di salute e altri dati di natura particolare

OPI Siena tratta, in modalità cartacea, dati idonei a rivelare lo stato di salute esclusivamente per finalità previste dalla legge che consistono essenzialmente:

a) Negli attestati di malattia relativi al personale dipendente consegnati o fatti pervenire all'ufficio o ai soggetti competenti;
b) Negli attestati di idoneità alla mansione relativi al personale dipendente rilasciati dal medico competente;
c) Altra documentazione personale fornita dagli iscritti.

La documentazione sanitaria relativa alla idoneità alla mansione riferita ai dipendenti è trattata, in conformità al D.Lgs. 81/2008 e s.m.i., in via esclusiva dal medico competente e viene conservata presso OPI Siena, in formato cartaceo all'interno di un contenitore dotato di serratura efficiente e sicura, nei modi e termini fissati dalla normativa citata.
I dati di cui alle precedenti lettere del presente paragrafo sono trattati, con un elevato grado di riservatezza, da personale appositamente incaricato e, al termine delle operazioni necessarie al raggiungimento della finalità, sono conservati unicamente per rispondere a obblighi normativi; nello specifico la conservazione dei dati particolari è fissata nel limite dei 10 anni. Una volta decorsi i termini indicati tali dati sono cancellati, distrutti o trasformati in forma non intelligibile.

10.6 Comportamenti virtuosi

Di seguito sono elencati i comportamenti virtuosi da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato particolare/sensibile deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati sensibili e/o alle categorie particolari di dati personali non devono essere lasciate su una scrivania non presidiata;
- i laptotp devono essere bloccati con un cavo di bloccaggio o conservati in un cassetto se non utilizzati;
- le password non possono essere lasciate su note adesive attaccate sopra, sotto o nei pressi di un computer, né

possono essere lasciate per iscritto in posizione accessibile;

- le stampe contenenti informazioni riservate e/o dati particolari/sensibili devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggidocumenti appositi;
- le lavagne contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere cancellate;
- i dispositivi portatili come laptop, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi;
- tutti i dispositivi di archiviazione di massa contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere conservati in cassetti chiusi a chiave.

Il dipendente che viola queste norme di comportamento è soggetto alle azioni disciplinari previste,
fino al licenziamento.

11 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

11.1 Titolare del trattamento

OPI Siena è il titolare del trattamento dei dati.
Gli artt. 24 e 25 del GDPR 2016/679 regolano le responsabilità del titolare del trattamento sulla conservazione, protezione e mantenimento dei dati personali in ordine al perseguimento delle sue finalità.

11.2 Responsabili del trattamento

Il titolare del trattamento ha individuato e nominato formalmente i responsabili esterni del trattamento controllando e verificando la loro attività.
Dato che OPI Siena si avvale per l'espletamento di alcune attività di soggetti esterni (persone fisiche o giuridiche) e considerato che tali soggetti trattano o hanno accesso a dati personali, questi sono stati nominati, dal titolare del trattamento, responsabili (esterni) del trattamento.

11.3 Autorizzati al trattamento

Il titolare del trattamento ha previsto, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo che specifici compiti e funzioni connesse al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità (art. 2-quaterdecies del D.Lgs. 101/2018).
Il titolare del trattamento ha individuato le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
Sono stati individuati quali "autorizzati al trattamento dati" i lavoratori dipendenti che effettuano trattamento, per la loro funzione, di dati personali.
Sono da considerarsi autorizzati a tutti gli effetti anche i dipendenti a tempo determinato, gli stagisti, i tirocinanti ed altri soggetti (persone fisiche) che effettuano trattamento, per il loro incarico, di dati personali.

Gli autorizzati sono nominati dal titolare del trattamento e sono indicati nell'Allegato 02 "Elenco personale autorizzato" del presente Modello Organizzativo.

11.4 Amministratore di sistema e manutentore informatico

Il titolare del trattamento individua e nomina formalmente i soggetti interni o esterni che svolgono attività di amministratori di sistema (Provvedimento a carattere generale - 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. n. 300 del 24 dicembre 2008).

Non è stato individuato un amministratore di sistema, bensì sono presenti dei tecnici informatici che svolgono attività di assistenza a chiamata (manutentore occasionale).

Questi sono:

- *la ditta che ha fornito il programma gestionale, che ha la possibilità di collegarsi con il server di OPI Siena e che si occupa anche di archiviare un back up dei dati dell'organizzazione;*
- *la Ditta/provider per la posta ed assistenza per connessione da remoto e per back up esterno dei dati dell'Ordine;*
- *la Ditta che ha fornito i computer e che offre assistenza per quanto riguarda i problemi al computer non legati al gestionale – fornitrice di programma antivirus;*

OPI Siena ha individuato e nominato formalmente i soggetti interni o esterni che svolgono attività di manutentori informatici, anche occasionali.

12 PROCEDURA DEL DIRITTO DI ACCESSO DELL'INTERESSATO

12.1 Procedura Per Il Diritto Di Accesso Dell'interessato

Il GDPR formalizza un ampio catalogo di diritti che spettano all'interessato.

Si tratta del diritto di accesso, del diritto di rettifica, del diritto alla cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul titolare.

È stata messa a punto una procedura che, a richiesta di un interessato, permette di rispondere tempestivamente ad una richiesta di accesso ai dati, fatte salve le eccezioni esplicitamente previste dal regolamento, come previsto dall'articolo 21 che illustra appunto tali eccezioni.

In risposta alle richieste di accesso, vengono di seguito esplicitamente illustrate le modalità con cui sono trattati i dati ed anche i soggetti terzi, ai quali tali dati possano essere eventualmente comunicati **entro 30 giorni dalla richiesta di accesso.**

12.2 Riscontro alla richiesta di accesso

Ogni richiesta di accesso deve essere codificata e registrata.

La richiesta di accesso deve essere accettata in forma scritta (la comunicazione potrà essere trasmessa in formato cartaceo o via e-mail).

La codifica data alla richiesta d'accesso sarà la seguente: **Rich-accesso_giorno-mese-anno-xx** dove xx sarà un numero progressivo a partire da 01.

In risposta alla richiesta scritta dell'interessato di accesso ai propri dati, il Titolare del trattamento metterà a disposizione dell'interessato tutte le informazioni richieste in un linguaggio chiaramente comprensibile, accompagnato da specifiche spiegazioni per facilitare la comprensione del messaggio da parte dell'interessato.

Nella risposta ad una richiesta di diritto di accesso, saranno anche indicate le modalità con cui l'interessato può reclamare nei confronti dell'accuratezza, l'aggiornamento e la completezza dei dati personali che lo riguardano, in modo da modificarli in modo appropriato.

Se la risposta alla richiesta il diritto di accesso dovesse essere negativa, verranno illustrate in dettaglio le ragioni per le quali non è in grado di soddisfare alla richiesta.

In considerazione all'articolo 18 del GDPR i dati saranno forniti all'interessato in forma scritta a lui indirizzata.

In conformità all'articolo 18 viene previsto anche che l'interessato possa chiedere al titolare del trattamento di comunicare direttamente i suoi dati ad un altro titolare; su richiesta dell'interessato verrà attuata questa richiesta.

COMUNICAZIONE PREVISTA NEL CASO DI RICHIESTA ESPRESSA DA PARTE DELL'INTERESSATO

Di seguito viene riportata la comunicazione prevista nel caso di richiesta espressa dall'interessato:

In riferimento al suo diritto di accesso previsto in materia di protezione dei dati personali, alla quale è stato assegnato il numero di riferimento ***Rich-accesso_giorno-mese-anno-xx***

Per dare seguito alla sua richiesta è necessario (riportare solo i casi che ricorrono):

- *Avere una prova della vostra identità, come effettivo interessato ai dati personali richiesti (si può richiedere una fotocopia della carta di identità, verificando che l'indirizzo di spedizione dei dati sia lo stesso indicato sulla carta di identità; si può accogliere una richiesta per posta elettronica, se firmata digitalmente)*
- *che il delegato, che ha presentato in suo nome la richiesta, fornisca un documento di legittimazione ad operare su incarico dell'interessato (indicare il documento di legittimazione richiesto; ad esempio, copia di lettera dell'interessato o atto notorio; per gli eredi, copia dell'atto di successione)*
- *che ci vengano indicati i seguenti ulteriori elementi, atti ad individuare con completezza ed accuratezza i dati personali di suo interesse (indicare ad es. il periodo, la natura dei dati, ecc.).*

Non appena riceveremo i documenti sopra indicati, sarà nostra cura rispondere entro 30 giorni dalla ricezione, segnalando che la risposta verrà inviata alla sua residenza anagrafica (od alla residenza anagrafica del delegato).

In alternativa, potrete ritirare la risposta presso la sede di OPI Siena negli orari di apertura al pubblico dell'Ordine.

Qualora la risposta alla vostra richiesta di diritto di accesso non fosse considerata da voi conforme potrete sporgere reclamo in forma scritta, al titolare del trattamento, in modo da permettere allo stesso la possibilità di fornire all'interessato una risposta esaustiva.

Se la risposta alla richiesta il diritto di accesso dovesse essere negativa, verranno illustrate in dettaglio le ragioni per le quali non è in grado di soddisfare alla richiesta.

La risposta verrà consegnata in busta chiusa all'interessato od a persona identificabile, in possesso di accettabile delega (precisare cosa si intende per accettabile, ad es. lettera con firma autenticata).

13 AFFRONTARE IL DATA BREACH (LA VIOLAZIONE DEI DATI)

Nel GDPR, l'articolo 31 e l'articolo 32 sono specialmente dedicati alle modalità con cui occorre affrontare una possibile violazione dei dati.

Il precedente del decreto legislativo 196 /2003 e successivi provvedimenti del garante aveva già reso obbligatoria la notificazione al garante di eventuali violazioni di dati, ma solo limitatamente ad alcune categorie di dati trattati ed alcuni tipi di titolari. Nel nuovo regolamento questo obbligo di notificazione è generalizzato, come previsto all'articolo 31comma 1.

L'obiettivo delle disposizioni dell'articolo 31 e dell'articolo 32 è quello di porre tempestivo riparo alle conseguenze, potenzialmente assai gravi, di una violazione di dati.

A questo proposito, occorre rilevare che le conseguenze della violazione di dati possono essere estremamente diversificate, in funzione del fatto che la violazione comporti la perdita di un dato, piuttosto che la sottrazione ed il possibile successivo utilizzo abusivo da parte di chi ha sottratto il dato.

Le disposizioni dei due articoli menzionati offrono tutt'una serie di indicazioni vincolanti, cui deve attenersi il Titolare ed il responsabile del trattamento, una volta rilevata una violazione dei dati.

L'articolo 31 comma 1 stabilisce che, se e quando si è verificata una violazione dei dati di tale violazione deve essere comunicata nel termine massimo di 72 ore da quando la violazione dei dati si è verificata, oppure dal momento in cui il data controller o data processor si è accorto di tale violazione.

Appare evidente che maggiore è questo intervallo massimo, maggiori sono le possibili conseguenze negative della violazione, in quanto una violazione dolosa permetterebbe a chi lo ha perpetrata di avere a disposizione un maggior tempo per utilizzare in modo improprio i dati stessi.

Inoltre, grazie all'articolo 32, è indispensabile stabilire modalità e tempi per la comunicazione della violazione ai soggetti interessati, onde anche essi possano eventualmente attivare misure di protezione, ad esempio in caso di furto di identità.

L'articolo 32 si preoccupa anche di fare presente che, anche in caso di violazione dei dati, potrebbe non essere necessaria la comunicazione agli interessati coinvolti, ove i dati violati siano comunque inutilizzabili per il perpetratore, ad esempio perché coperti da protezione criptografica.

13.1 Procedure per la gestione del data breach

Ogni autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il Titolare del trattamento.

Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale data breach, predispone la comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

Ogniqualvolta il titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto.

Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach1.

Ad ogni responsabile del trattamento deve essere comunicato il contatto del titolare del trattamento al quale effettuare la predetta segnalazione.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato	Caratteristiche: Dati non recuperabili o provenienti da procedure non ripetibili	Smarrimento di chiavetta USB contenente dati originali Smarrimento di fascicolo cartaceo del personale dipendente	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Caratteristiche: Dati non recuperabili o provenienti da procedure non ripetibili. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	Guasto non riparabile dell'hard disk. Incendio di archivio cartaceo.	Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia). Rottura di un PC che non contiene dati personali originali (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Caratteristiche: Modifiche sistematiche su più casi. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Guasto tecnico che altera parte dei contenuti, compromettendo anche i backup. Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema, rilevato e sanato tramite operazioni di recovery. Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile. Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Malfunzionamento del sistema di Consegna di dati ad altri senza autorizzazione	Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet. Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche autorizzati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete istituzionale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi Accesso non autorizzata di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti dall'ordine	Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup cancellazione accidentale dei dati da parte di una persona non autorizzata perdita della chiave di decrittografia di dati crittografati in modo sicuro.	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso.

13.2 Traccia di comunicazione di violazione dei dati

Il titolare del trattamento predispone la comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Nella comunicazione devono essere riportate le seguenti informazioni:

- Indicare il nome dell'organizzazione
- Indicare il nominativo della persona di contatto
- Indicare se si è avuto già occasione di segnalare in precedenza incidenti della stessa natura.
- Dare indicazione di quando si è verificato l'incidente.
- Descrivere sinteticamente l'incidente
- Dare una traccia dei dati personali coinvolti
- Dare indicazione di quanti interessati sono stati coinvolti
- Indicare se gli interessati sono stati informati
- Dare informazione se sono state intraprese misure per ridurre o mitigare gli effetti della perdita dei dati.
- Indicare se si è condotta un'inchiesta interna sull'accaduto.
- Dare indicazione sulle azioni intraprese per prevenire il ripetersi di simili incidenti in futuro.

14 OBBLIGHI NEI CONFRONTI DELL'INTERESSATO E DELL'AUTORITÀ GARANTE

14.1 Informativa

L'informativa deve essere, secondo quanto scritto nell'art. 12 del GDPR 2016/679, concisa, trasparente e semplice da interpretare.
L'informativa deve fornire, secondo quanto scritto nell'art. 13 del GDPR 2016/679, i dati di titolare e responsabili del trattamento, le finalità del trattamento, i destinatari, il periodo di conservazione, i diritti dell'interessato.
Il titolare del trattamento adotta tre distinte tipologie di informativa che, preventivamente, fornisce alle proprie categorie di interessati: *i dipendenti o soggetti assimilati, agli iscritti ed ai fornitori.*
L'informativa contiene tutti gli elementi di cui all'art. 13 del GDPR 2016/679 e all'art. 13, comma 1, del D.lgs. 196/2003 e viene:

a) Consegnata, in forma scritta ai dipendenti al momento dell'assunzione (firma del contratto);
b) Consegnata agli iscritti o richiedenti l'iscrizione prima dell'inizio del trattamento dei dati;
c) Consegnata ai fornitori al momento della sottoscrizione di contratti/convenzioni/incarichi o, in assenza di questa documentazione, consegnata assieme alla accettazione del preventivo di spesa;

Nelle e-mail utilizzate per l'esercizio dell'attività lavorativa è opportuno che venga riportata una informativa breve sul trattamento dei dati i cui contenuti possono essere quelli di cui al modulo (Allegato D) allegato al presente Modello Organizzativo.

INFORMATIVA SULLA PROTEZIONE DATI AI SENSI art. 13 RGPD UE 2016/679

(Iscritti all'Ordine)

Scopo del presente documento, **in qualità di iscritto o richiedente iscrizione all'Ordine delle Professioni Infermieristiche di Siena è quello di informarla**, su quali siano i suoi dati che trattati dall'ordine, quali siano le finalità per cui vengono trattati ed eventualmente condivisi, per quanto tempo vengono conservati, quali sono i suoi diritti come interessato e come può esercitarli.

Titolare del trattamento è l'Ente "Ordine delle Professioni Infermieristiche di Siena" (OPI Siena) che agisce per tramite del Consiglio e nella persona del suo legale rappresentante, il Presidente di OPI Siena dott. Francesco D'Ambrosio domiciliato per carica presso la l'Ente stesso e che opera anche quale Responsabile del Trattamento.

QUALI DATI PERSONALI CHE RIGUARDANO PERSONE FISICHE POSSONO ESSERE RACCOLTI

1) **Dati fiscali, di identità, altri dati personali comuni** ed altre informazioni o documenti relativi ai requisiti per la prima iscrizione e per il mantenimento dell'iscrizione all'albo quali residenza, cittadinanza, diplomi e crediti relativi a percorsi formativi, pagamento di quote o tasse di iscrizione. Dati relativi a corsi e altri servizi o consulenze forniti da OPI Siena o da terzi e da Lei richiesti e/o utilizzati.
2) **Dati Sensibili di tipo giudiziario,** relativi al casellario giudiziario in caso di richiedenti prima iscrizione o, nel caso di soggetti già iscritti, a seguito di procedimenti disciplinari attivati da OPI Siena o in base a richieste degli enti giudiziari o di polizia in relazione a indagine penale, civile o amministrativa.
3) **Dati relativi alle procedure di cui all'art. 4 D.L. n. 44/2021, convertito, con modifiche, dalla L. n. 76/2021, come modificato dal D.L. n. 172/2021.**

OPI Siena NON raccoglie nessun dato ai fini di controllo o profilazione dell'interessato.

COME VENGONO RACCOLTI I DATI PERSONALI

1) Dati personali comuni forniti dall'interessato o da soggetti da esso delegati

I dati possono essere raccolti nelle seguenti modalità:

- attraverso l'inserimento dei dati e l'invio della richiesta di informazioni dai siti internet collegati al nostro Ente o attraverso e-mail, posta o altri canali di informazione e comunicazione;
- mediante trasmissione e/o consegna effettuata dall'interessato stesso alla nostra sede direttamente o tramite intermediario per l'evasione di una richiesta di informazioni, di un servizio o di un adempimento;
- nell'ambito di attività connesse all'esecuzione di adempimenti, servizi o in relazione ai rapporti economici o istituzionali intrattenuti con l'interessato.

2) Dati Sensibili giudiziari raccolti da OPI Siena in fase di prima iscrizione

Si tratta di dati e certificazioni richiesti al casellario giudiziario per il perfezionamento della pratica richiesta dall'interessato.

3) Dati Sensibili forniti da altri enti o soggetti nell'ambito di istruttorie disciplinari o procedimenti giudiziari

In questo si tratta di dati sensibili di tipo giudiziario, sanitario e altri dati personali utilizzati a seguito di procedimenti disciplinari o di indagini penali, civili o amministrative.

Per le nuove iscrizioni, i dati particolari trattati potrebbero essere raccolti direttamente presso l'interessato ovvero, ove consentito, con le modalità descritte al paragrafo relativo all'origine dei dati.

Tali dati particolari non sono trasmessi a terzi destinatari, mentre i dati comuni potrebbero essere inviati ai destinatari a cui debbano essere trasmessi nel rispetto delle disposizioni vigenti in tema di diniego o accoglimento delle istanze di iscrizione agli albi ed elenchi speciali ad esaurimento degli Ordini delle professioni sanitarie.

La comunicazione ditali da parte dell'interessato costituisce un obbligo legale; in caso di mancata comunicazione degli stessi, non sarà possibile procedere all'iscrizione.

FINALITA' E PRESUPPOSTO DEL TRATTAMENTO CUI SONO DESTINATI I DATI PERSONALI

I dati personali degli iscritti o richiedenti iscrizione potranno essere trattati per:

1) **L'adempimento ad obblighi previsti da leggi, da regolamenti o da altre norme, da provvedimenti dell'autorità giudiziaria, ovvero in base ad obblighi contabili, retributivi, assistenziali o fiscali (Art. 6 c. 1 lett. c, lett. e RGPD).**

La principale attività dell'Ordine delle Professioni Infermieristiche è la tenuta dell'Albo professionale: ne consegue, ai sensi ai sensi dell'art. 9 del DLCPS 233/46 e art. 4 del DPR 221/50 e norme successive, l'esigenza di acquisire e trattare i dati personali degli iscritti, di darne la pubblicità derivante dalla natura di pubblico registro dell'Albo, attuare la vigilanza sul rispetto del codice deontologico, curare la formazione permanente e la partecipazione degli iscritti alla formazione ed al funzionamento degli organi; fornire agli iscritti i servizi previsti dalle norme di legge, dallo statuto e in esecuzione di delibere degli organi dell'Ente.

Rientrano tra dette attività istituzionali anche:

- l'informazione agli iscritti relativa alle attività dell'Ente, alla loro partecipazione alla formazione ed al funzionamento degli organi dell'Ordine, a norme, circolari e documentazione relativa alle professioni infermieristiche e all'ambito sanitario di interesse per gli associati.
- L'informazione e la promozione in relazione a attività formative, servizi o nuove iniziative rientranti tra le finalità dell'Ente e da questo organizzate o patrocinate.

Rientrano in questa finalità i dati relativi alle procedure di cui all'art. 4 D.L. n. 44/2021, convertito, con modifiche, dalla L. n. 76/2021, come modificato dal D.L. n. 172/2021. Il trattamento è realizzato per l'assolvimento delle disposizioni della citata normativa di cui all'art. 1 D.L. n. 172/2021 e sue eventuali ss.mm.ii., in esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri attribuiti alla scrivente ed agli Ordini delle Professioni Infermieristiche territoriali ed essendo il trattamento necessario per motivi di interesse pubblico rilevante sulla base della norma in parola, consistenti nel fine di assolvere al ruolo di enti sussidiari dello Stato nella specie deputati a consentire di "*tutelare la salute pubblica e mantenere adeguate condizioni di sicurezza nell'erogazione delle prestazioni di cura e assistenza*" (cfr. art. 1, comma 1, d.l. n. 172/2021).

Qualora l'interessato intenda iscriversi o mantenere l'iscrizione all'Albo, il conferimento dei dati personali necessari a tali finalità è obbligatorio ed il relativo trattamento non richiede il consenso dell'interessato.

Sarà invece **cura dell'interessato collaborare per mantenere i dati corretti e aggiornati,** *segnalando tempestivamente errori o modifiche* che dovessero interessare i propri dati.

Per tali attività verranno utilizzati i dati ed i canali di comunicazione già acquisiti dall'Ente nei rapporti istituzionali con l'interessato, attraverso lettere, telefono, posta elettronica o altri strumenti di comunicazione.

2) **Finalità connesse all'esecuzione di attività formative, di consulenza o altri servizi o altri rapporti di natura contrattuale che l'interessato ha richiesto o ai quali ha aderito (Art. 6 c. 1 lett. b RGPD)**.

Il conferimento dei dati personali necessari a tali finalità non è obbligatorio, ma il rifiuto di fornirli può comportare, in relazione al rapporto tra il dato e l'adempimento richiesto, l'impossibilità dell'Ente di eseguire l'attività stessa o parte di essa o di adempiere a richieste specifiche dell'interessato preliminari all'esecuzione della richiesta o alla conclusione di un contratto. *Qualora tali dati vengano forniti, il consenso al loro trattamento si ritiene implicito nella richiesta dell'interessato.*

3) **Altre informazioni e comunicazioni non istituzionali (Art. 6 c. 1 lett. a RGPD).**

Rientrano in questa categoria:

- **l'informazione e la promozione relativa a iniziative, corsi, convegni e altre attività formative o culturali organizzate da soggetti terzi e/o promossa da OPI Siena;**
- l'informazione su concorsi, selezioni e altre opportunità di lavoro professionale o a titolo di volontariato pervenute o segnalate a OPI Siena;
- la diffusione dei propri dati personali comuni, previa richiesta, tramite pubblicazione sul sito istituzionale OPI Siena.

Per tali attività verranno utilizzati i dati ed i canali di comunicazione già acquisiti dall'Ente nei rapporti istituzionali con l'interessato, attraverso lettere, telefono, posta elettronica o altri strumenti di comunicazione.

Il conferimento dei dati personali necessari a tali finalità non è obbligatorio e il loro trattamento richiede uno specifico consenso.
Qualora l'interessato voglia opporsi al trattamento dei propri dati in relazione a queste finalità, può farlo in qualunque momento, mediante semplice richiesta scritta o via e-mail a paograz.gp@pec.libero.it **inviata al Responsabile Protezione Dati (RPD) incaricato dott.ssa Paola Graziani presso l'Ordine delle Professioni infermieristiche di Siena** – Viale Europa, 31 53100 Siena (SI), **specificando il tipo di trattamento ed il canale attraverso il quale non desideri più essere contattato.**
Tale revoca non pregiudica la liceità del trattamento basato sul consenso precedentemente prestato.

COOKIE POLICY

OPI Siena utilizza per il proprio sito istituzionale unicamente cookie c.d. "tecnici": si tratta di cookie che servono a effettuare la navigazione o fornire un servizio richiesto dall'utente.

NON si impiega nessun cookie ai fini di controllo o profilazione dell'interessato.

Per ulteriori dettagli si rimanda alla cookie policy presente sul sito www.opisiena.it/.

PER QUANTO TEMPO CONSERVIAMO I DATI PERSONALI

I dati personali vengono conservati solo per il tempo necessario al conseguimento delle finalità per le quali sono stati raccolti o per qualsiasi altra legittima finalità collegata.

Se i dati personali sono trattati per due o più finalità, essi verranno conservati fino a che non sarà cessata la finalità con il termine di conservazione previsto più lungo. I dati personali che non siano più necessari o per i quali non vi sia più un presupposto giuridico per la relativa conservazione vengono anonimizzati irreversibilmente (e in tal modo potranno essere conservati) o distrutti in modo sicuro.

Salvo che la legge non imponga specifiche esigenze di conservazione, i dati personali sono conservati **per l'intera durata dell'iscrizione e per un termine ulteriore pari a 10 anni e sei mesi dall'estinzione del rapporto**, in considerazione dei termini di prescrizione di diritti od obblighi in relazione ai quali l'Ente potrebbe avere necessità di difendersi o adempiere o delle esigenze di conservazione imposte dalla normativa.

Con riferimento **ai dati funzionali all'instaurazione del rapporto, laddove non perfezionato, gli stessi saranno conservati per un termina massimo di 12 mesi**, al fine di consentirci di poter rispondere a specifiche richieste dell'interessato.

I dati giudiziari degli interessati vengono conservati per un periodo di 6 mesi, dopo il completamento delle procedure di iscrizione o per le quali vengono raccolti e trattati e vengono poi distrutti in modo sicuro.

I dati relativa alle procedure di cui all'art. 4 d.l. n. 44/2021, convertito, con modifiche, dalla l. n. 76/2021, come modificato dal d.l. n. 172/2021.

La durata del trattamento coincide con la vigenza della normativa citata di cui all'art. 1 d.l. n. 172/2021 e sue eventuali ss.mm.ii.

Per i termini di conservazione dei soli dati necessari ad attivare le procedure di cui all'art. 4, comma 3, d.l. n. 44/2021, convertito, con modifiche, dalla l. n. 76/2021, come modificato dal d.l. n. 172/2021 – con ciò riferendosi ai dati relativi ai soggetti non vaccinati, come risultanti dalla Piattaforma nazionale-DGC e dalla eventuale documentazione dai

medesimi prodotta – deve farsi riferimento a quanto necessario per il perseguimento delle finalità in esame, nel rispetto di quanto previsto in tema di obblighi per gli archivi storici.
Non è prevista la conservazione dei dati rilevanti relativi a coloro che siano risultati in regola con l'obbligo vaccinale mediante la consultazione automatizzata della piattaforma nazionale-DGC.

SICUREZZA DEI DATI PERSONALI

OPI Siena utilizza tutte le misure di sicurezza necessarie al miglioramento della protezione ed al mantenimento della sicurezza, dell'integrità e dell'accessibilità dei dati personali raccolti.
Tutti i dati personali sono conservati su server protetti o documenti cartacei idoneamente archiviati o su altri supporti elettronici (server, cloud, ecc.) di nostri fornitori di servizi che sono stati specificamente autorizzati al trattamento e sono accessibili in base ai nostri standard e alle nostre policy di sicurezza o standard equivalenti. Il dettaglio delle modalità tecniche e organizzative per il trattamento e le relative misure di sicurezza è disponibile, a richiesta, presso l'Ente stesso – Titolare del trattamento.

ACCESSO AI DATI PERSONALI E/O CONDIVISIONE CON ALTRI SOGGETTI

Ai dati personali possono avere accesso i consiglieri di amministrazione ed i dipendenti debitamente autorizzati, nonché i fornitori esterni nominati, se necessario, responsabili del trattamento, che forniscono supporto per l'erogazione dei servizi.
Tale trattamento verrà effettuato, per conto di OPI Siena – per le medesime finalità e con le modalità sopra descritte.
L'elenco di detti enti, società o imprese è disponibile presso la sede dell'Ente stesso o può essere richiesto **m**ediante semplice richiesta scritta o via e-mail inviata al Responsabile Protezione Dati (DPO) incaricato dott.ssa Paola Graziani presso l'Ordine delle Professioni infermieristiche di Siena.
In relazione alla normativa vigente, i medesimi dati sono messi a disposizione del pubblico mediante accesso regolato e comunicati alle altre autorità ed amministrazioni pubbliche con le quali l'Ordine si rapporta per esigenze di pubblico interesse, in base alle norme che regolano le professioni infermieristiche.
Solo su specifica richiesta dell'interessato, una parte limitata dei propri dati comuni potrà essere diffusa attraverso l'inserimento nell'elenco dei professionisti pubblicato sul sito istituzionale OPI Siena. Con la diffusione dei propri dati personali, OPI Siena non avrà più alcun controllo sui dati diffusi e tali dati potrebbero essere utilizzati da soggetti terzi, anche in paesi Extra UE, anche per finalità diverse da quelle previste con la pubblicazione.
Il titolare non trasferisce i dati personali in Paesi nei quali non è applicato il RGPD (paesi extra UE) salvo specifiche indicazioni contrarie per le quali verrà preventivamente informato e, se necessario, acquisito il consenso.

DIRITTI DELL'INTERESSATO IN MATERIA DI PROTEZIONE DEI DATI E DI AVANZARE RECLAMI DINNANZI ALL'AUTORITÀ DI CONTROLLO

Come previsto dal RGPD, l'interessato ha il diritto di chiedere all'Ente:

- l'accesso ai Suoi dati personali;
- la copia dei dati personali che Lei ci ha fornito (c.d. portabilità);
- la rettifica dei dati in nostro possesso,
- la cancellazione di qualsiasi dato per il quale non abbiamo più alcun presupposto giuridico per il trattamento;
- l'opposizione al trattamento ove previsto dalla normativa applicabile;
- la revoca del consenso, nel caso in cui il trattamento sia fondato sul consenso;
- la limitazione del modo in cui vengono trattati i Suoi dati personali, nei limiti previsti dalla normativa a tutela.

Tali diritti possono essere esercitati mediante richiesta scritta inviata al Responsabile Protezione Dati (RPD) incaricato dott.ssa Paola Graziani presso l'Ordine delle Professioni infermieristiche di Siena– Viale Europa 31, Cap. 53100 SIENA (SI) o a mezzo mail: paograz.gp@pec.libero.it.

Tali diritti soggiacciono ad alcune eccezioni finalizzate alla salvaguardia dell'interesse pubblico (ad esempio, il non esercizio della professione infermieristica ai fini della cancellazione dall'Albo) e degli altri interessi pubblici e dell'Ente.

Nel caso in cui l'interessato esercitasse uno qualsiasi dei summenzionati diritti, sarà nostro onere verificare che sia legittimato ad esercitarlo, dando riscontro, di regola, entro un mese.

In relazione alle segnalazioni o richieste circa il trattamento dei Suoi dati faremo ogni sforzo per rispondere alle sue preoccupazioni.

Tuttavia, nel caso non avesse riscontro o se lo desidera, Lei potrà inoltrare i propri reclami o le proprie segnalazioni al Garante per la protezione dei dati personali – Piazza di Monte Citorio n. 121 – 00186 ROMA.

15 ANALISI DEI RISCHI DPIA

Secondo l'art. 35 del GDPR 2016/679, "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".

La valutazione d'impatto sulla protezione dei dati di cui al presente paragrafo è richiesta se esiste una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione; se il trattamento è su larga scala di categorie particolari di dati personali di cui all'art. 9 comma 1 del GDPR 2016/679; se esiste una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

16 CONTROLLI E VERIFICHE

16.1 Controllo e verifica da parte del titolare del trattamento

Il titolare del trattamento, in riferimento all'attività svolta dai responsabili esterni, verifica periodicamente la puntuale osservanza delle istruzioni impartite, attraverso nomina formale, da parte dei responsabili.

Il titolare del trattamento verifica ed aggiorna almeno annualmente la lista dei responsabili esterni del trattamento riscontrando l'ambito di trattamento consentito.

Resta fermo che il titolare del trattamento potrà organizzare verifiche periodiche dell'operato dei responsabili in riferimento al trattamento dati di loro competenza nei modi che riterrà opportuni anche ricorrendo a visite di controllo.

Il titolare del trattamento verifica ed aggiorna almeno annualmente la lista degli autorizzati di trattamento riscontrando l'ambito di trattamento consentito ed i relativi profili di autorizzazione.

17 Conservazione della documentazione

Il titolare del trattamento istituisce ed aggiorna un fascicolo dove conserva il presente documento e tutta la documentazione relativa alla materia in oggetto.

18 ALLEGATI

18.1 Allegato A

PROCEDURA DI BACKUP	
DESCRIZIONE RUOLI E RESPONSABILITÀ	
Ruolo	***Descrizione delle responsabilità***
Titolare del trattamento	Dispone o effettua le operazioni necessarie al salvataggio dei dati, anche avvalendosi dell'intervento di soggetti esterni o di personale interno e, se del caso, vigila sull'operato dei soggetti preposti alle operazioni di salvataggio dei dati.
Incaricato al trattamento	Effettua le operazioni necessarie al salvataggio dei dati che gli sono state formalmente assegnate dal titolare o dal responsabile del trattamento dati.
DESCRIZIONE FLUSSO DELLE PROCEDURA	
a) In relazione alle caratteristiche del sistema informatico, all'evoluzione tecnologica e ad una valutazione del rapporto costi/benefici viene individuata la soluzione tecnologica per realizzare il backup nel rispetto delle disposizioni normative. b) In funzione della soluzione tecnologica individuata vengono acquisite e rese operative le risorse (hardware e/o software) necessarie. c) Viene definita la lista dei dati oggetto del salvataggio. d) Viene stabilito che l'esito della verifica di leggibilità dei dati memorizzati nei supporti sia verbalizzato. e) Viene individuato un luogo sicuro, diverso dalla sala macchine, e un contenitore idoneo (cassaforte/armadio blindato) dotato di serratura efficientemente sicura dove conservare i supporti rimovibili di memorizzazione in cui vengono salvati i dati. f) Vengono individuati formalmente i soggetti autorizzati di effettuare le operazioni comprese nella presente procedura, specificando per ciascuno analiticamente i compiti e le istruzioni da seguire.	
DESCRIZIONE DELLE RISORSE	
Risorse tecnologiche	Dotazioni software e hardware necessarie in funzione della soluzione tecnologica adottata per realizzare il backup nel rispetto delle disposizioni normative.
Risorse umane	Soggetti interni e/o esterni individuati formalmente attraverso nomina scritta.

18.2 Allegato B

PROCEDURA DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE E DEI PROFILI DI AUTORIZZAZIONE	
DESCRIZIONE RUOLI E RESPONSABILITÀ	
Ruolo	***Descrizione delle responsabilità***
Titolare del trattamento	Dispone o effettua le operazioni necessarie alla gestione (attribuzione, cambio, revoca) degli account, delle password e dei profili di autorizzazione ad essi associati, anche avvalendosi dell'intervento di soggetti esterni o di personale interno e, se del caso, vigila sull'operato dei soggetti preposti alle operazioni di salvataggio dei dati.
Incaricato al trattamento	Effettua le operazioni necessarie alla gestione (attribuzione, cambio, revoca) delle credenziali di autenticazione e dei profili di autorizzazione ad essi associati che gli sono state formalmente assegnate.
DESCRIZIONE FLUSSO DELLE PROCEDURA	

a) La password di accesso ed i profili di autorizzazione ad essa associati vengano assegnati all'incaricato all'atto del primo conferimento dell'incarico.
b) La password è modificata dall'incaricato al primo utilizzo e, successivamente, almeno **ogni sei mesi**.
c) In caso di trattamento di categorie particolari di dati la password è modificata almeno ogni **tre mesi.**
d) La parola non deve contenere riferimenti agevolmente riconducibili all'incaricato e, se il sistema lo consente, deve essere composta da almeno 8 caratteri in caso contrario deve contenere un numero di caratteri pari al massimo consentito.
e) In caso di perdita della password da parte dell'incaricato oppure in caso di mancato utilizzo dei codici identificativi da parte dello stesso, per oltre sei mesi, le credenziali verranno disattivate.
f) Le credenziali di accesso verranno registrate e conservate in una busta che verrà successivamente sigillata ed opportunamente identificata e custodita;
g) In caso di prolungata assenza o impedimento da parte dell'incaricato che renda indispensabile accedere alle credenziali dello stesso, adeguatamente custodite, sarà avvertito tempestivamente l'incaricato interessato delle necessità di OPI Siena.

Gli autorizzati del trattamento sono stati istruiti sul contenuto della procedura e sulle regole da seguire in riferimento alla sua applicazione;

Sono stati individuati i soggetti autorizzati di effettuare le operazioni comprese nella presente procedura, specificando per ciascuno analiticamente i compiti e le istruzioni da seguire.

DESCRIZIONE DELLE RISORSE	
Risorse tecnologiche	Dotazioni software e hardware eventualmente necessarie in funzione della soluzione tecnologica adottata per la gestione (attribuzione, cambio, revoca) degli account, delle password e dei profili di autorizzazione ad essi associati.
Risorse umane	Soggetti interni e/o esterni individuati formalmente attraverso nomina scritta.

18.3 Allegato C

PROCEDURA DI GESTIONE DEI SISTEMI DI SICUREZZA (HW E SW)	
DESCRIZIONE RUOLI E RESPONSABILITÀ	
Ruolo	***Descrizione delle responsabilità***
Titolare del trattamento	Dispone o effettua le operazioni necessarie alla gestione dei sistemi di sicurezza (HW e SW) anche avvalendosi dell'intervento di soggetti esterni o di personale interno e, se del caso, vigila sull'operato dei soggetti preposti alle operazioni di salvataggio dei dati.
Incaricato al trattamento	Effettua le operazioni necessarie alla gestione dei sistemi di sicurezza (HW e SW) che gli sono state formalmente assegnate.
DESCRIZIONE FLUSSO DELLE PROCEDURA	

a) In relazione alle caratteristiche del proprio sistema informatico, all'evoluzione tecnologica e ad una valutazione del rapporto costi/benefici individua la soluzione tecnologica per realizzare un livello di sicurezza adeguato nel rispetto delle disposizioni normative.

b) In funzione della soluzione tecnologica individuata vengono acquisite e rese operative le risorse (hardware e/o software) necessarie.

c) Vengono definiti i seguenti parametri relativi alla gestione dei sistemi di sicurezza (HW e SW):

Risorse tecnologiche adottate	Antivirus presente sui server e sui client. Firewall a protezione dell'intero sistema informatico.
Aggiornamento delle risorse	Le risorse software sono aggiornate automaticamente ogni qualvolta siano disponibili nuovi aggiornamenti online. Le risorse hardware verranno aggiornate quando risultano superate a livello tecnologico o recuperate/sostituite in caso di malfunzionamenti.

d) Vengono individuati i soggetti autorizzati di effettuare le operazioni comprese nella presente procedura, specificando per ciascuno analiticamente i compiti e le istruzioni da seguire.

DESCRIZIONE DELLE RISORSE	
Risorse tecnologiche	Dotazioni software e hardware necessarie in funzione della soluzione tecnologica adottata per la protezione del sistema informatico.
Risorse umane	Soggetti interni e/o esterni individuati formalmente attraverso nomina scritta.

18.4 Allegato D

Di seguito vengono riportati i modelli di informativa Privacy da inserire nelle mail in uscita:

Informativa Privacy mail in uscita

Informativa Privacy - Ai sensi del Regolamento (UE) 2016/679 si precisa che le informazioni contenute in questo messaggio sono riservate e ad uso esclusivo del destinatario. Qualora il messaggio in parola. Le fosse pervenuto per errore, La preghiamo di eliminarlo senza copiarlo e di non inoltrarlo a terzi, dandocene gentilmente comunicazione. Grazie.
Privacy Information - This message, for the Regulation (UE) 2016/679, may contain confidential and/or privileged information. If you are not the addressee or authorized to receive this for the addressee, you must not use, copy, disclose or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by reply e-mail and delete this message. Thank you for your cooperation.

Informativa Privacy nel caso di invio di moduli di raccolta dati personali via e-mail

Informativa ai sensi Art. 13 Regolamento Europeo (EU) 2016/679
Il Titolare del trattamento è OPI Siena che ha sede in Viale Europa, 31 Cap. 53100 Siena (SI).
Per qualsiasi necessità, in materia di trattamento dei dati personali, lei potrà contattare il Titolare del trattamento, nella persona del Dott. Francesco D'Ambrosio, all'indirizzo e-mail: *presidente@opisiena.it*.
I suoi dati personali verranno trattati con strumenti informatici da personale autorizzato dal Titolare, per la gestione delle sue richieste.
I suoi dati saranno trattati per avviare, istruire e chiudere procedimenti di natura amministrativa
Questi non saranno comunicati a terzi a meno che la base giuridica del loro trattamento non sia il rispetto di un adempimento legislativo regolamentato per la tenuta e la gestione dell'Albo a seguito di iscrizioni, modifiche di informazioni, cancellazioni e sanzioni disciplinari.
I dati saranno conservati per il tempo necessario alla loro gestione.
Lei potrà esercitare i diritti previsti dal Regolamento UE 2016/679 in materia di rettifica, cancellazione, blocco, portabilità dei dati.

Informativa Privacy Fatture, Ddt, etc.

Trattiamo i Vostri dati per fini amministrativi
e contabili. Li tuteliamo rispettando la
Privacy e a richiesta rimettiamo Informativa
completa ai sensi del Regolamento (UE) 2016/679

Informativa Privacy in comunicazioni riservate

Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

Le informazioni contenute nella presente e-mail ed in ogni eventuale file allegato sono riservate e comunque destinate esclusivamente alla persona o all'ente sopra indicato.

La diffusione, distribuzione, la copiatura della e-mail trasmessa da parte di persona diversa dal destinatario non sono consentite, salvo autorizzazione espressa.

Non permettendo Internet di assicurare l'integrità del presente messaggio, si declina ogni responsabilità in merito, nell'ipotesi in cui esso venga modificato.

Se avete ricevuto questa e-mail per errore vi preghiamo di eliminarla dai vostri archivi e darne comunicazione al mittente.