ORDINE DEI FARMACISTI DELLA PROVINCIA DI PISA
56121 – Pisa - Via U. Aldrovandi, 3 tel. 050/9657355
e-mail: info@ordinefarmacisti.pisa.it
Pec: ordinefarmacistipi@pec.fofi.it
Sito: www.ordinefarmacisti.pi.it
Codice Fiscale 80007550504

ORDINE FARMACISTI PISA

Norme e disposizioni

in applicazione del

Regolamento Generale sulla Protezione dei Dati personali

(Regolamento UE 679/2016 - di seguito indicato "RGPD"),
del Codice in materia di protezione dei dati personali 196/03 modificato dal decreto 101 del 2018
e successive modifiche, integrazioni.

Presidente e Legale Rappresentante dell'Ordine.	Dr. Enrico Morgantini

Referente per il trattamento dei dati	Dr.ssa Nadia Pierrette Campilongo

Responsabile della protezione dei dati (DPO)	Calzolari Tonino

Versione Documento	1.0	**Data Versione**	24/9/2018
Descrizione modifiche	**1’ rilascio**		
Motivazioni	**Norme e disposizioni per il trattamento dei dati personali**		

Redatto in bozza da:	Calzolari Tonino – DPO SSP
Validato da:	Segretario del Consiglio
Approvato da:	Consiglio dell’Ordine
Conservato presso:	ORDINE di Pisa
Tipologia di documento:	Regolamento
Destinatari/Utilizzatori	Interna all’ente

INDICE:

Finalità

Il presente Regolamento rappresenta uno strumento di sensibilizzazione, informazione e formazione del personale dipendente nonché degli eventuali collaboratori che intervengono nei trattamenti dei dati.

E' stato redatto allo scopo di:

a. definire comportamenti corretti, in linea con le disposizioni del Consiglio dell'Ordine;
b. rendere consapevoli coloro che operano in nome e per conto dell'Ordine di poter provocare, anche involontariamente, un illecito passibile di sanzioni rilevanti;
c. confermare che l'Ordine non tollera comportamenti illeciti, di qualsiasi tipo, anche se la stessa fosse in condizione di trarne vantaggio;
d. prevenire rischi, assicurare i diritti degli interessati e rispettare la normativa in argomento.

Tutto il personale dipendente ed i collaboratori nello svolgimento delle attività di competenza sono tenuti a rispettarlo scrupolosamente.

Il mancato rispetto o la violazione delle disposizioni in materia potranno essere perseguiti con provvedimenti disciplinari nonché con azioni civili e penali previste dalla normativa vigente.

Definizioni

Ai fini del Regolamento si applicano le definizioni di cui all'art. 4 del RGPD e/o le definizioni riportate nel Glossario seguente.

Entrata in vigore e pubblicità

Il presente Regolamento modifica e sostituisce le precedenti comunicazioni/disposizioni in materia.

Il testo viene consegnato ad ogni dipendente o collaboratore all'inizio del rapporto di lavoro e resta a disposizione del personale nell'archivio dell'Ordine.

Si invita tutto il personale, dopo un'attenta lettura a restituire la scheda riportata sull'ultima pagina debitamente compilata e sottoscritta.

Aggiornamento e revisione

Il presente Regolamento è soggetto ad aggiornamento e revisione periodica, ogni incaricato può suggerire al responsabile della protezione dei dati dell'Ordine modifiche o integrazioni al presente testo.

Responsabilità nell'applicazione del RGPD

Il testo del RGPD introduce un nuovo approccio, sulla responsabilizzazione **dell'ORDINE Titolare del trattamento e sui suoi referenti interni,** in quanto grava su di Loro l'onere della prova relativamente alla liceità ed all'adeguatezza del trattamento (Principio di Accountability).

È quindi compito dell'Ordine Titolare dei dati assicurare la definizione, l'applicazione, il controllo delle misure di sicurezza necessarie ed essere in grado di produrre documentazione adeguata relativamente alle valutazioni eseguite sui rischi derivanti dai trattamenti.

Allo scopo quindi d'informare i dipendenti e i collaboratori sulle caratteristiche essenziali da applicare ai trattamenti e tradurre in istruzioni e/o disposizioni operative quanto previsto della norma, si dispone quanto nel seguito indicato.

Misure di sicurezza "adeguate" e Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

Il principio-chiave è garantire la protezione dei dati già in fase di ideazione e progettazione di un trattamento o di un sistema (**«privacy by design»)**.

La normativa in argomento, impone al Titolare di mettere in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio per i diritti e le libertà delle persone fisiche.

Evidente quindi la necessità da parte del Titolare e del Responsabile del trattamento di definire un sistema di controllo e valutazione, che consenta di adeguare le misure di sicurezza ai potenziali rischi derivanti e mantenerne il controllo nel tempo.

Costruzione del SGSI e sua applicazione

L'organizzazione, l'attivazione ed il controllo del SGSI, per mantenere il livello di rischio accettabile dall' Ordine è di competenza del Consiglio dell'Ordine e del suo Presidente che, tramite il Responsabile Interno ha il compito di definire:

- ✧ **organigramma e responsabilità:** per una chiara ed organica attribuzione dei compiti - prevedendo, per quanto possibile, una segregazione delle funzioni o, in alternativa, dei controlli compensativi - nonché a controllare la correttezza dei comportamenti;
- ✧ **disposizioni/regole** volte a definire processi e procedure per un'adeguata gestione e valutazione delle attività e dei rischi;
- ✧ **formazione dei dipendenti ed informazione ai collaboratori;**
- ✧ **sistema di controllo** in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità**.**

DISPOSIZIONI GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

I dipendenti incaricati al trattamento di dati personali ricevono istruzioni dal Responsabile Interno del trattamento, adeguata formazione con manuali operativi e regolamenti/disposizioni aziendali.

I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati (devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»));

e) 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.

f) trattati in maniera da garantire un'adeguata sicurezza mediante misure tecniche e organizzative appropriate. («integrità, disponibilità e riservatezza»).

Per la gestione dei dati deve sussistere almeno **una delle seguenti condizioni**:

a) l'interessato ha espresso il consenso al trattamento;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di attività precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

Il personale nell'espletamento del proprio lavoro deve:

- osservare il più rigoroso segreto d'ufficio;
- garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati non coerente con le disposizioni ricevute;
- non comunicare ad altri e non portare all'esterno dell'ambiente di lavoro documenti e/o supporti magnetici contenenti dati, se non in presenza di una specifica autorizzazione del Titolare o del Responsabile Interno dell'Ordine;
- raccogliere dati personali solo dopo aver fornito all'interessato adeguata informativa per i trattamenti eseguiti e ove ne ricorrano gli obblighi, aver ottenuto dallo stesso adeguato consenso al trattamento.

Chiunque dovesse ricevere una richiesta scritta da un interessato, che intende far valere i propri diritti relativamente al trattamento dei dati che lo riguardano, previsti dagli artt. 15-21 del RGPD (ad esempio: conferma di quanto eseguito, richiesta di rettifica, cancellazione, opposizione e/o limitazione del trattamento), **deve informare tempestivamente il Responsabile Interno**

dell'Ordine, che provvederà se del caso, a coinvolgere il Consiglio ed il Responsabile della protezione dei dati (c.d. DPO) dell'Ordine.

Registro delle attività di trattamento (art. 30 e cons. 171)

Il RGPD impone la tenuta di un registro aggiornato relativo alle attività di trattamento eseguite.

La redazione del registro è obbligatoria soltanto in ipotesi determinate, ma è uno **strumento ritenuto indispensabile e fondamentale dall'azienda,** in quanto permette al Titolare di:

- mantenere aggiornata la mappa dei trattamenti e dei dati trattati;
- individuare i trattamenti che comportano rischi per i diritti e le libertà personali degli interessati
- mantenere evidenza dei principali interventi eseguiti nelle attività di trattamento.

Il registro dei trattamenti deve riportare le principali caratteristiche delle attività eseguite (finalità, riferimenti dei Titolari, Responsabili, descrizione delle categorie dei dati e degli interessati, le categorie di destinatari cui è prevista la comunicazione, la tipologia degli asset utilizzati, le misure di sicurezza applicate, tempi di conservazione, la formazione impartita agli incaricati e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte).

Viene incaricato dell'aggiornamento e della conservazione del registro dei trattamenti il Responsabile Interno dell'Ordine, con la collaborazione degli amministratori dei sistemi informatici ed il coinvolgimento tecnico di StudioFarma.

L'aggiornamento sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, la piena conformità dei trattamenti in corso (cons. 171).

Per i trattamenti che presentano un rischio elevato per i dati trattati o per un'eventuale non conformità alle normative dovrà essere coinvolto nell'analisi il RPD (Responsabile della Protezione dei dati) ed il Consiglio dell'ORDINE ed il presidente (per l'accettazione del rischio).

L'attività dovrà essere tracciabile e saranno mantenute adeguate evidenze delle valutazioni eseguite.

TRATTAMENTO ELETTRONICO DEI DATI

ACCESSO ALLE INFORMAZIONI RESIDENTI SU ARCHIVI ELETTRONICI

L'accesso ai sistemi informatici dell'Ordine, avviene mediante credenziali di identificazione basate su un codice personale "USER-ID" e da una parola chiave o password che in autonomia ogni incaricato deve personalizzare in sede di prima abilitazione e variare con cadenza massima definita. La credenziale di accesso dell'utente "USER-ID" è rappresentato da un codice alfanumerico, conosciuto dall' Ordine e riconducibile all'incaricato a cui il codice è stato assegnato.

Detti codici hanno lo scopo di:

a. riconoscere il dipendente o collaboratore che si connette ai sistemi;
b. determinare il profilo di autorizzazione e i dati a cui può accedere;
c. identificare le attività svolte nella sessione di lavoro.

L'inserimento di un codice personale e l'attribuzione delle relative autorizzazioni deve essere:

a. richiesto dal Responsabile Interno dell'Ordine o da un suo sostituto/fiduciario;
b. inserito nei vari ambienti dagli amministratori dei sistemi incaricati alla gestione;
c. segnalato all'incaricato (dipendente o collaboratore/collaboratore) che dovrà modificare immediatamente la password di accesso assegnata assumendo la titolarità dell'utenza.

Il dipendente o collaboratore è responsabile di ogni eventuale improprio utilizzo.

La credenziale di accesso di un dipendente/collaboratore, che non ha più la necessità di accedere al sistema (cessazione rapporto di lavoro), deve essere immediatamente revocata/bloccata da parte dell'Amministratore del sistema, dietro tempestiva segnalazione del Responsabile Interno dell'Ordine.

Istruzioni per il corretto utilizzo di "USER-ID" e Password/parola chiave

Ogni incaricato (dipendente/collaboratore) che si connette ad un sistema con la propria "USER-ID" deve completare il riconoscimento mediante la digitazione della propria parola chiave (password).

La biunivocità "USER-ID – Parola chiave" consente di identificarlo e consentirgli l'accesso alle risorse a cui è autorizzato per la mansione svolta, secondo le modalità operative previste.

La parola chiave costituisce il meccanismo fondamentale del sistema di controllo degli accessi e pertanto deve essere gestita con la massima diligenza e segretezza.

Al fine di proteggere la segretezza della parola chiave è necessario attenersi alle istruzioni nel seguito riportate.

La parola chiave è strettamente personale, deve essere custodita con la massima cura e non va assolutamente comunicata ad alcuno, per nessun motivo, anche se richiesta.

La prima assegnazione della parola chiave all'utente avviene contestualmente all'attribuzione della "USER-ID" da parte dei gestori dei vari sistemi.

Tale parola chiave deve essere cambiata dall'incaricato (dipendente/collaboratore), al primo accesso, prima che lo stesso possa svolgere qualsiasi altra operazione.

Successivamente alla prima personalizzazione, la parola chiave rimane di esclusiva responsabilità e gestione del dipendente/collaboratore, che può modificarla ogni qualvolta ritenga che la stessa abbia perso le caratteristiche di riservatezza.

La lunghezza della parola chiave deve essere almeno di 8 caratteri (si evidenzia che il livello di sicurezza degli accessi aumenta con la lunghezza e la complessità della stessa).

La parola chiave può essere composta da caratteri alfabetici, numerici, speciali; deve contenere contemporaneamente sia numeri che lettere, non può essere uguale al nome o al cognome dell'incaricato.

La nuova parola chiave deve essere creata nella maniera più casuale possibile e nel rispetto della regola che vieta l'utilizzo di parola chiave corrispondenti alle ultime 3 utilizzate.

Si raccomanda di evitare codici chiave facilmente scopribili: "banali" di soli numeri o lettere sequenziali, password simili alla "USER-ID" o con riferimenti a entità facilmente intuibili associate all'incaricato stesso (es. parte del nominativo proprio o dei familiari con numero di sequenza, ecc.).

Il cambio della credenziale di identificazione (password) richiede la digitazione corretta della precedente, la digitazione della nuova, nonché la ri-digitazione di quest'ultima per conferma.

La digitazione della parola chiave avviene in maniera nascosta/mascherata allo scopo di evitarne l'individuazione da parte di eventuali osservatori, si raccomanda di evitare l'inserimento quando si è osservati.

Le parole chiave sono memorizzate nel sistema in modo "crittografato", per garantirne la massima riservatezza. Si raccomanda di non annotare la propria parola chiave in luoghi facilmente accessibili (es. sul P.C., sul manuale delle istruzioni, ecc.). Nel caso si voglia conservarne traccia scritta, per propria memoria, essa deve essere conservata con cura e in luogo chiuso.

E' opportuno variare la parola chiave di frequente in modo da evitare che altri la possano scoprire. In particolare, è consigliabile cambiare la password ogniqualvolta si tema che possa essere stata individuata anche fortuitamente da qualcuno e con maggiore frequenza in occasione dello svolgimento di lavori particolarmente riservati.

Il sistema considera valida una parola chiave aggiornata negli ultimi 90 giorni, altrimenti obbliga a variare il codice al primo collegamento effettuato dopo tale periodo. Se la durata di inattività supera i 180 giorni scatta il blocco automatico dell'utente (User-ID), con conseguente impossibilità da parte dello stesso di svolgere qualsiasi altra operazione. Per l'eventuale riattivazione, si dovrà contattare l'amministratore del sistema interessato.

In caso di dimenticanza del codice chiave o di errori commessi in occasione dell'ultima variazione, l'utente deve richiedere all'amministratore del sistema interessato, in modo tracciabile, la riassegnazione di una nuova parola chiave. Ottenuto il nuovo codice, si dovrà accedere al sistema secondo le modalità previste per la "prima assegnazione" (immediata personalizzazione del codice stesso).

Il sistema dopo 10 immissioni errate della parola chiave revoca automaticamente la relativa USER-ID. Per ottenere il ripristino della "USER-ID" revocata, occorre inoltrare formale richiesta al Responsabile dei sistemi informativi, indicandone la motivazione.

In caso di abbandono della propria postazione di lavoro, è obbligatorio che l'utente chiuda la sessione di lavoro.

TRATTAMENTO DI DATI PERSONALI RESIDENTI SUI SERVER

L'accesso alle risorse presenti sui Server, è protetto con "USER-ID" e password personali, attribuite, controllate e gestite con le regole sopra descritte.

Le autorizzazioni di accesso ai dati personali sono attribuite dagli amministratori delle credenziali di accesso a seguito delle richieste del Responsabile Interno dell'Ordine, in funzione della mansione svolta dall'incaricato.

Gli amministratori del sistema sono tenuti a:

a) verificare almeno settimanalmente la pubblicazione di eventuali nuove vulnerabilità segnalate nei siti di riferimento delle aziende fornitrici del Software e dopo adeguato ri-collaudo funzionale dei sistemi, applicare le modifiche indicate per rimuovere dette vulnerabilità;

b) mantenere traccia delle modifiche applicate e delle variazioni delle misure minime di sicurezza.

E' vietato disattivare il programma antivirus sui sistemi ed è vietato caricare qualsiasi tipo di programma e/o archivio dati che non siano strettamente connessi all'attività lavorativa.

E' compito degli Amministratori dei sistemi, in accordo con il Responsabile Interno dell'Ordine, provvedere/disporre al fine di:

- far eseguire giornalmente copia di sicurezza dei dati;
- conservare i supporti magnetici in locali separati dagli elaboratori, in contenitori ad accesso controllato;
- controllare periodicamente la funzionalità e la disponibilità dei salvataggi;
- definire la durata per la conservazione dei salvataggi e smagnetizzare e/o distruggere i supporti al termine del loro utilizzo;
- verificare la cancellazione dei dati presenti su disco fisso in caso di cessato utilizzo dell'apparecchiatura;
- registrare su apposito registro degli incidenti, ogni problema/rischio, incidente, modifica rilevante del sistema utilizzato nel trattamento dei dati;
- depositare in busta chiusa sicura la password amministrativa dei sistemi;
- relazionare periodicamente al Responsabile della Protezione dei Dati (RPD/DPO) circa eventuali incidenti accorsi e/o suggerire miglioramenti delle regole di sicurezza applicate.

L' Amministratore del Sistema Informatico, per ovviare a situazioni di pericolo e/o rischio derivanti da attacchi informatici (es. Virus, spyware, worm, ecc.) deve effettuare periodicamente (almeno annualmente) verifiche e controlli necessari per individuare possibili vulnerabilità dei sistemi.

L'Ordine si riserva la facoltà, anche senza preavviso, di accedere ai dati presenti nei sistemi e procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la Sicurezza o la funzionalità/disponibilità dei servizi gestiti.

Tutti gli incaricati sono tenuti alla cancellazione dei file obsoleti o inutili per l'attività svolta.

UTILIZZO DI PERSONAL COMPUTER CONNESSI IN RETE

Il Computer affidato al dipendente o collaboratore dall'Ordine è uno strumento di lavoro, pertanto ne è vietato l'utilizzo per attività non attinenti allo svolgimento delle proprie mansioni.

Ogni attività di configurazione e installazione di nuovi software sui sistemi viene eseguita dal personale incaricato; senza l'esplicita e preventiva autorizzazione da parte dell'Amministratore dei Sistemi, **non è consentito all'utente assegnatario della risorsa** di:

- installare autonomamente e/o utilizzare programmi provenienti dall'esterno;
- utilizzare e/o memorizzare programmi e/o files audio o video personali (immagini, filmati e file musicali personali);
- trattare (memorizzare, elaborare, conservare) in autonomia dati dell'Ordine;
- installare sul proprio PC dispositivi di memorizzazione, comunicazione (come ad esempio smartphone, masterizzatori, chiavette USB, supporti magnetici esterni) non forniti dall'Ordine;
- disattivare il prodotto antivirus e/o altri prodotti di sicurezza utilizzati (firewall, log);
- modificare le caratteristiche impostate sul proprio PC (indirizzo IP, politiche di sicurezza).

Il Computer deve essere spento al termine dell'attività lavorativa svolta, in caso di assenze prolungate dalla postazione di lavoro deve essere sconnesso dalla sessione remota o attivato lo screen saver con relativa password.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema Informatico nel caso in cui vengano rilevati virus.

I supporti magnetici contenenti dati sensibili e giudiziari, devono essere criptati o custoditi inderogabilmente all'interno degli uffici dell'Ordine, in archivi protetti ad accesso controllato.

Sarà cura degli amministratori del sistema eseguire e verificare l'applicazione delle politiche sopra indicate e l'aggiornamento automatico delle impronte virali relative al programma antivirus.

UTILIZZO DI PC PORTATILI e Dispositivi Mobili (SmartPhone, Tablet)

L'utente è responsabile degli apparati che gli sono stati assegnati dall'Ordine e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi mobili (PC portatili, SmartPhone, Tablet) si applicano le regole di utilizzo previste per i sistemi connessi in rete.

Sarà compito dell'amministratore dei sistemi attivare programmi di tracciatura dell'attività, protezione e controllo, tali da garantire la necessaria sicurezza dei dispositivi, la protezione dei dati e la possibilità di analizzare le cause in caso d'incidenti e/o malfunzionamento dei sistemi.

USO DELLA POSTA ELETTRONICA

La casella di posta elettronica eventualmente assegnata all'utente dall'Ordine è uno strumento di lavoro, gli assegnatari sono responsabili del corretto utilizzo della stessa.

È vietato utilizzare la posta elettronica (salvo diversa ed esplicita autorizzazione del Responsabile Interno dell'Ordine) per l'invio di messaggi personali, per la partecipazione a forum/chat personali.

La casella di posta deve essere visionata con frequenza, mantenuta in ordine, cancellando documenti inutili/obsoleti e soprattutto allegati ingombranti.

Per comunicazioni interne preferire l'uso di caselle d'ufficio a quelle personali.

In caso di assenza prolungata dell'utente, attivare messaggi automatici che segnalino al mittente il periodo di assenza e a chi rivolgersi per eventuali urgenze, oppure individuare un fiduciario dipendente o collaboratore che possa accedere alla casella di posta elettronica personale in caso di urgenza.

I contenuti delle caselle di posta dell'ufficio, rimangono consultabili per due anni, vengono copiati annualmente in supporti informatici estraibili ed archiviati per 10 anni in ambiente protetto.

USO DELLA RETE INTERNET

L'accesso alla rete internet per l'incaricato viene richiesto dal Responsabile Interno dell'Ordine all'amministratore dei sistemi, che provvederà ad eseguire le opportune abilitazioni e ad informare il dipendente/collaboratore stesso.
Il sistema di collegamento ad Internet è uno strumento di lavoro, pertanto ne è vietato l'utilizzo per attività non attinenti allo svolgimento delle proprie mansioni.
Se non espressamente autorizzati dal Responsabile Interno dell'Ordine, è vietato:

- navigare in siti non attinenti allo svolgimento delle proprie mansioni;
- partecipare o collegarsi per motivi non professionali a forum, chat-line, banche elettroniche, blog, sondaggi, ecc.;
- registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- scaricare files o programmi non aventi alcuna attinenza con le mansioni assegnate, anche se gratuito (freeware e shareware).

È altresì vietato:

- trasmettere, diffondere/pubblicare documenti informatici di natura discriminatoria, oltraggiosa, diffamatoria, oscena, ingiuriosa, offensiva, illecita o contenente dati personali specie se sensibili;
- effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Responsabile Interno dell'Ordine e con il rispetto delle previste procedure di acquisto.

Utilizzo di sistemi cloud

È vietato agli incaricati la memorizzazione dei dati nei sistemi cloud, anche se gratuiti, se non espressamente e preventivamente approvati dall'Ordine.

Diritto d'autore

È vietato utilizzare programmi e dati in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248).
In particolare, è vietato utilizzare materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato.

Restituzione dei device

A seguito di una cessazione del rapporto lavorativo o al venir meno dei presupposti per l'utilizzo dei device dell'Ordine (ad insindacabile giudizio dell'Ordine), gli incaricati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei device in uso;
2. divieto assoluto di copiare, formattare, cancellare, alterare o manomettere i sistemi e/o i dati in essi contenuti.

Distruzione dei Device

Ogni device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti al Responsabile Interno dell'Ordine che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

TRATTAMENTO DI DATI PERSONALI RESIDENTI SU ARCHIVI CARTACEI

Gli atti e i documenti contenenti dati personali e/o sensibili (vedi definizioni seguenti) devono essere conservati in contenitori/armadi o locali con accesso limitato al personale incaricato.

I documenti cartacei, se contenenti dati personali, dovranno essere trattati in modo riservato e distrutti previa autorizzazione dell'apposita direzione dell'Archivio generale dello Stato.

È vietata la stampa e/o la riproduzione di documenti se non finalizzate all'attività lavorativa.

Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o al venir meno presupposti per l'utilizzo dei documenti (ad insindacabile giudizio dell'Ordine), gli incaricati hanno i seguenti obblighi:

1. procedere immediatamente alla restituzione dei documenti in loro possesso;
2. divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

AMMINISTRATORE DEI SISTEMI

Questa funzione è svolta da OLIVIO GHILARDUCCI (Lunet) in qualità di Responsabile di trattamento.

Tra i suoi compiti sono compresi quelli di documentare, coordinare e controllare l'esecuzione di:

- configurazioni dei sistemi in ottemperanza delle disposizioni impartite dal Responsabile Interno dell'Ordine e delle normative/disposizioni dell'Ente;
- interventi HW da parte dei manutentori del sistema;
- salvataggi dei dati in accordo con il Responsabile Interno dell'Ordine.

Deve inoltre:

- collaborare per aggiornare il registro dei trattamenti ed individuare misure adeguate a garantire la continuità dei servizi, la riservatezza delle informazioni e la disponibilità/funzionalità dei sistemi;
- verificare e rimuove le vulnerabilità pubblicate dalle società fornitrici dei sistemi utilizzati;
- verificare l'aggiornamento delle impronte virali del prodotto antivirus utilizzato;
- verificare la validità/certificazione e/o la necessità di adeguare il prodotto antivirus utilizzato;
- verificare la vulnerabilità dei portali collegati ad internet.

Per ogni sistema installato negli uffici dell'Ordine, deve modificare la password di "default" per l'accesso al sistema, inserirla in una busta chiusa sigillata, firmarla e consegnarla al Responsabile Interno del'Ordine.

Addetti alla gestione di user-id e password

La mansione è svolta dalla **Sig.ra Donatella Barontini** per i seguenti sistemi aziendali:
Server della Lan, Proxy di collegamento ad Internet / intranet, Portale.

Tra i loro compiti sono compresi quelli di:

- inserire, modificare e/o revocare credenziali di identificazione (User-Id e password);
- inserire o modificare i profili utente, attribuendo le autorizzazioni sulla base delle formali richieste dei responsabili delle unità organizzative;
- verificare periodicamente (al massimo ogni sei mesi) le credenziali presenti nel sistema e le relative autorizzazioni;
- predisporre ogni sei mesi l'elenco delle credenziali attive e delle relative autorizzazioni;
- revocare i diritti di accesso al personale e/o ai collaboratori a seguito della richiesta del Responsabile Interno dell'Ordine e comunque alla cessazione del rapporto lavorativo o, al venir meno dei presupposti per l'accesso ai sistemi e/o all'utilizzo di dati cartacei.

Obbligo di comunicare i casi di violazione dei dati personali (data breach)

Il titolare del trattamento (per il tramite del suo Presidente, con la collaborazione del Consiglio dell'Ordine e del Responsabile Interno) deve comunicare eventuali violazioni dei dati personali all'Autorità Garante della protezione dei dati.

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine); oppure, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato, la comunicazione avviene sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

Gestione dei rischi e degli incidenti

Ogni dipendente o collaboratore è tenuto a segnala~~re~~ tempestivamente al Responsabile Interno dell'Ordine, in forma tracciabile (ad esempio utilizzando le caselle di posta) eventuali violazioni nelle misure di sicurezza, smarrimento o furto di informazioni o di strumenti informatici, trattamenti illeciti o situazioni di rischio di cui sia venuto a conoscenza.

Per ogni incidente, si dovrà procedere con una prima rapida valutazione dell'accaduto e dei rischi derivanti.
In seguito, **l'amministratore del sistema di riferimento, dovrà:**

- **raccogliere la documentazione comprovante quanto accaduto;**
- **conservarla in modo da garantirne la disponibilità, l'integrità e per quanto possibile, evitare ogni contestazione da parte degli incaricati.**

Nel caso in cui l'incidente abbia compromesso o possa compromettere la riservatezza, l'integrità o la disponibilità dei dati, dovrà essere coinvolto tempestivamente il "Responsabile della Protezione dei dati" ed il Consiglio dell'Ordine, che provvederà ad indicare:

- le contromisure da attivare;
- l'obbligo di notificazione all'Autorità Garante;
- l'obbligo di comunicazione tempestiva agli interessati coinvolti.

AUDIT e CONTROLLI ESEGUITI

Controlli periodici vengono eseguiti dal Responsabile Interno e dall'amministratore del sistema informatico, ognuno per quanto di competenza, per verificare e garantire la corretta applicazione delle disposizioni e delle procedure definite dal Titolare e raggiungere gli obiettivi indicati.

I controlli da eseguire sono concordati con il Presidente dell'Ordine Titolare e la scelta deve tenere in considerazione la legislazione vigente e le situazioni di rischio evidenziate nei trattamenti.

I risultati dei controlli sono riportati dal Responsabile Interno al Consiglio che pianifica le attività di riduzione e/o eliminazione dei rischi rilevati.

Vengono eseguiti almeno ogni 6 mesi i seguenti controlli:

Descrizione	
Funzionalità, adeguatezza e aggiornamento degli strumenti elettronici utilizzati al fine di proteggere i dati dal rischio di intrusione o perdita.	SI
Aggiornamento delle "patch" di sicurezza dei sistemi e dei programmi per computer utilizzati.	SI
Integrità, funzionalità e disponibilità dei salvataggi e delle istruzioni organizzative e tecniche affinché gli stessi siano effettuati almeno settimanalmente.	SI
Persistenza e adeguatezza dei diritti di accesso ai dati ed ai sistemi per tutti gli incaricati in possesso di credenziali attive, rispetto le mansioni svolte.	SI
Avvenuta formazione per i dipendenti/collaboratori incaricati del trattamento e gestione del PIANO DI FORMAZIONE dell'Ente.	NO

Viene verificata ad inizio di ogni trattamento ed in occasione dell'aggiornamento del registro dei trattamenti:

l'adeguatezza delle misure di sicurezza adottate e la valutazione dei rischi per gli interessati, derivante dal trattamento dei dati personali.	SI

Periodicamente inoltre vengono eseguite attività di controllo non programmate, da parte del responsabile della protezione dei dati.

SANZIONI

Le sanzioni amministrative sono disciplinate dagli articoli 83 e 84 del RGPD.

Ogni autorità di vigilanza (in Italia il Garante della protezione dei Dati) assicura, in ogni caso, che la sanzione sia **effettiva, proporzionata e dissuasiva**, secondo i seguenti parametri:

- la natura, la gravità e la durata della violazione, anche in considerazione del numero degli interessati e dei danni da questi subiti;
- il carattere intenzionale o colposo dell'infrazione;
- le azioni intraprese dal Titolare o dal Responsabile per mitigare i danni subiti dagli interessati;
- il grado di responsabilità del Titolare o del Responsabile, anche sotto il profilo tecnico, e le misure organizzative attuate per prevenire le violazioni;
- eventuali rilevanti violazioni precedenti da parte del Titolare o del Responsabile;
- il livello di cooperazione con l'autorità di vigilanza, al fine di porre rimedio alla violazione e mitigarne i possibili effetti negativi;
- le categorie di dati personali oggetto della violazione;
- l'adesione a codici di condotta o a meccanismi di certificazione riconosciuti;
- ogni altro fattore aggravante o attenuante applicabile alle circostanze del caso;
- i benefici finanziari ottenuti, o le perdite evitate, direttamente o indirettamente, per effetto della violazione commessa.

Se il Titolare o il Responsabile hanno commesso, intenzionalmente o per negligenza, più violazioni alle disposizioni del Regolamento connesse a una stessa operazione di trattamento di dati personali, l'importo totale della sanzione non dovrà superare l'importo indicato per la violazione più grave.

Sono soggette a sanzioni amministrative fino a 10 milioni di euro, o fino al 2% del fatturato totale annuo mondiale dell'esercizio precedente se superiore, le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui agli articoli:

- 10 (trattamenti che non richiedono l'identificazione degli interessati),
- 23 (privacy by design e privacy by default),
- 24 (contitolarità del trattamento),
- 26 (Responsabili del trattamento),
- 27 (istruzioni e autorità del Titolare),
- 28 (documentazione relativa a ciascun trattamento di dati personali),
- 29 (cooperazione con l'autorità di vigilanza),
- 30 (sicurezza del trattamento),
- 31 (notificazione dei data breach all'autorità),
- 32 (comunicazione dei data breach agli interessati),
- 33 (DPIA – Data Protection Impact Assessment),
- 34 (consultazione preventiva dell'autorità di vigilanza),
- 35, 36 e 37 (designazione, posizione e compiti del DPO – Data Protection Officer),
- 39 e 39a (processi di certificazione).

Sanzioni amministrative fino a 20 milioni di euro, o fino al 4% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, sono invece previste per le violazioni in materia di principi base del trattamento, condizioni per il consenso, diritti degli interessati, trasferimento di dati personali all'estero, mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza.

I profili di responsabilità comunque sono e restano tre: penale, amministrativo e civile.

L'ampiezza dell'ambito civile/risarcitorio è dettata dal paragrafo 1 dell'articolo 82, che recita:
"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.".

Regolamento approvato nella seduta del Consiglio Direttivo in data 17/02/2020.

Presidente ***Dr. Enrico Morgantini***

Vicepresidente ***Dr.ssa Giuseppina Mariani***

Tesoriere ***Dr. Andrea Cammilli***

Segretario ***Dr.ssa Nadia Pierrette Campilongo***

Consigliere ***Dr.ssa Letizia Cellai***

Consigliere ***Dr. Antonio Bottari***

Consigliere ***Dr. Simone Sbrana***

Consigliere ***Dr.ssa Alina Ranzani***

GLOSSARIO per gli Ordini dei Farmacisti

Ai fini del presente "Regolamento" valgono le stesse definizioni previste nell'art 4 della normativa in argomento. Più in particolare s'intende per:

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

LIMITAZIONE DI TRATTAMENTO»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

PROFILAZIONE: qualsiasi forma di trattamento di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

PSEUDONOMIZZAZIONE: il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

ARCHIVIO: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

TITOLARE DEL TRATTAMENTO»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Nello specifico l'Ordine Provinciale dei Farmacisti

RESPONSABILE DEL TRATTAMENTO»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

RESPONSABILE INTERNO: Nello specifico il Responsabile Interno dell'Ordine o altra figura designata al ruolo con delibera del Consiglio dell'Ordine

RESPONSABILE ESTERNO: persona fisica o giuridica che svolge il trattamento dei dati del Titolare con parziale autonomia.

DESTINATARIO: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;

INTERESSATO: la persona fisica cui si riferiscono i dati;

CONSENSO DELL'INTERESSATO: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

VIOLAZIONE DEI DATI PERSONALI: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

DATI GENETICI: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

DATI BIOMETRICI: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

DATI RELATIVI ALLA SALUTE: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

CREDENZIALI DI AUTENTICAZIONE: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

PAROLA CHIAVE: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

PROFILO DI AUTENTIFICAZIONE: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

SISTEMA DI AUTENTIFICAZIONE: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.