REGOLE DI COMPORTAMENTO PER IL PERSONALE DIPENDENTE
E I SOGGETTI AUTORIZZATI AL TRATTAMENTO
DEI DATI PERSONALI
MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI:
LINEE GUIDA, ISTRUZIONI OPERATIVE, OBBLIGHI

1 PREMESSA

Il presente Regolamento è emanato ai sensi della vigente normativa in materia di protezione dei dati personali delle persone fisiche, nazionale ed europea, con particolare riferimento al Regolamento Europeo 2016/679 in materia di protezione dei dati personali (nel seguito "Regolamento UE") – e completa ogni altra procedura interna dell'Ordine l'Ordine dei Medici Chirurghi ed Odontoiatri della provincia di AREZZO ("Ente") per i trattamenti e la protezione dei dati personali, con particolare riferimento alle misure di sicurezza poste a tutela dei trattamenti effettuati sia con strumenti elettronici e sia con atti e documenti cartacei, in originale e in copia, disposti in archivi fisici.

L'uso delle tecnologie informatiche, ed in particolare l'accesso alla rete Internet, espone il datore di lavoro a possibili rischi di natura patrimoniale e giuridica, con conseguenze sul piano della sicurezza, del patrimonio e dell'immagine dell'Ente.

Tenuto conto che l'utilizzo delle risorse informatiche e telematiche da parte del personale deve sempre ispirarsi al principio della diligenza e correttezza, dell'Ente attraverso il presente regolamento ha adottato una serie di norme interne, dirette ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Tali prescrizioni integrano le specifiche istruzioni fornite a tutti gli Autorizzati in attuazione della normativa in materia di protezione dei dati personali.

2 INFORMAZIONI GENERALI SULLA PROTEZIONE DEI DATI PERSONALI

Il diritto alla protezione dei dati è un diritto fondamentale dell'uomo, previsto all'art.1 del Regolamento UE e al Considerando (1) ed all'art. 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea come all'art. 16, paragrafo 1, del Trattato sul funzionamento dell'UE stabiliscono che "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*".

Si ricorda preliminarmente che la normativa attuale, introduce il principio di responsabilizzazione e rendicontazione del Titolare il quale in maniera proattiva sceglie autonomamente le misure di sicurezza adeguate, per la protezione dei dati personali trattati all'interno della propria organizzazione, le quali devono essere periodicamente aggiornate dallo stesso anche in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Le misure di sicurezza poste a tutela dei dati costituiscono un obbligo finalizzato alla protezione dei dati.

Il trattamento dei dati personali richiede obbligatoriamente l'adozione di idonee e preventive misure di sicurezza. Chiunque essendovi tenuto, omette di adottarle, è suscettibile di sanzioni amministrative, civili e penali e, nell'ambito di un rapporto di lavoro, anche sanzioni disciplinari.

Le misure di sicurezza che sono prescritte dal Titolare **riguardano il complesso delle misure tecniche, informatiche, organizzative, fisiche, logistiche e procedurali** che configurano i livelli di protezione necessari a ridurre o mitigare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Di seguito sono riportati i principali concetti e definizioni che il Regolamento UE elenca all'art. 4.

3 PRINCIPALI CONCETTI E DEFINIZIONI

Si intende per:
"**DATO PERSONALE**", qualunque informazione relativa a persona fisica, identificata o identificabile ("interessato"), anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. I dati personali come ad esempio: il nome, il cognome, il codice fiscale, la residenza, il numero di cellulare, la casella di posta, l'indirizzo Internet, l'indirizzo IP, il saldo del conto corrente, le credenziali di accesso al sito, ecc. sono considerati "dati comuni". Tra i dati personali sono definiti "**dati particolari**"quei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

"**TRATTAMENTO**", qualunque operazione o complesso di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali, concernenti la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, la selezione, l'estrazione, l'utilizzo, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il blocco, la comunicazione, la diffusione, il raffronto o l'interconnessione, la limitazione, cancellazione o la distruzione.

"**PROFILAZIONE**" qualsiasi forma di trattamento automatizzato per la raccolta di dati personali utilizzata per valutare comportamenti, aspetti personali, abitudini, usi, rendimento professionale, situazione economica, salute, interessi e preferenze.

"**PSEUDONIMIZZAZIONE**" trattamento di dati personali svolto in modo tale che questi dati non possano essere attribuiti all'interessato specifico senza l'utilizzo di informazioni aggiuntive a condizione che tali informazioni siano separate e soggette a misure intese a garantire che tali dati personali non siano attribuiti direttamente all'interessato.

"**CONSENSO**" manifestazione di volontà, libera, specifica, informata ed inequivocabile.

"TITOLARE DEL TRATTAMENTO", la persona fisica, la persona giuridica, la pubblica amministrazione, l'ente o altro organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità e i mezzi del trattamento di dati personali.

"RESPONSABILE", la persona fisica o la persona giuridica, l'autorità pubblica, l'ente o altro organismo che tratta dati personali per conto del titolare al trattamento.

"AUTORIZZATI", le persone fisiche autorizzate a compiere operazioni di trattamento del dato dal titolare o dal responsabile.

"INTERESSATO", la persona fisica a cui si riferiscono i dati personali.

"**DESTINATARIO**" la persona fisica o la persona giuridica, l'autorità pubblica, l'ente o altro organismo che riceve comunicazione di dati personali.

"GARANTE", l'autorità di controllo disciplinata all'articolo 51 del Regolamento UE.

Per quanto attiene più specificatamente alla sicurezza dei dati e dei sistemi, il Regolamento UE prescrive all'artt. 24, 25 e 32 che il titolare e il responsabile del trattamento mettono in atto misure, tecniche ed organizzative adeguate, per garantire un livello di sicurezza adeguato al rischio. In particolare al quarto comma dell'art. 32 è previsto che gli stessi garantiscano che chiunque agisca sotto la loro autorità, e abbia accesso ai dati personali non tratti tali dati se non è istruito in tal senso.

Relativamente alle misure di sicurezza, in relazione ai fini del presenta atto sono da definirsi:

"MISURE ADEGUATE", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello adeguato di protezione richiesto in relazione ai rischi previsti nell'articolo 32.

"STRUMENTI ELETTRONICI", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

"AUTENTICAZIONE INFORMATICA", l'autenticazione è il processo attraverso il quale viene verificata l'identità di un utente che vuole accedere ad un computer o ad una rete. È il sistema che verifica, effettivamente, che un individuo è chi sostiene di essere. L'autenticazione è diversa dall'identificazione (la determinazione che un individuo sia conosciuto o meno dal sistema) e dall'autorizzazione (il conferimento ad un utente del diritto ad accedere a specifiche risorse del sistema, sulla base della sua identità).

"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 AUTORIZZAZIONE", 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 AUTORIZZAZIONE", 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.

4 DISPOSIZIONI GENERALI

Il presente Regolamento costituisce la disciplina dell'Ente per i trattamenti dei dati personali, con particolare riferimento alle misure di sicurezza poste a tutela dei trattamenti effettuati:

- Con strumenti elettronici (prevalentemente computer, sia se operanti in modalità stand alone, sia se connessi in rete);
- Senza l'ausilio di strumenti elettronici (prevalentemente atti e documenti cartacei detenuti su archivi fisici).

Tutto il personale dipendente, i consulenti, i collaboratori esterni occasionali, gli addetti alla manutenzione e gestione di strumenti elettronici, le persone in *stage* sono tenuti a rispettarlo scrupolosamente, nell'ambito delle proprie competenze ed attività.

La violazione parziale o totale delle norme contenute nel Regolamento potrà essere suscettibile di provvedimenti disciplinari commisurati alla gravità della violazione, oltre che alle sanzioni civili, penali nonché disciplinari previste dalla vigente normativa.

Si dispone, inoltre, che copia del presente regolamento venga consegnato:

- All'atto dell'assunzione o dell'avvio del rapporto di collaborazione, ad ogni nuovo dipendente o collaboratore;
- Durante le sessioni formative di aggiornamento;
- All'atto della definizione del contratto, ai collaboratori esterni ed ai consulenti che operano internamente all'organizzazione;
- Pubblicato nella sezione Amministrazione trasparente, nella sezione "Altri Contenuti".

Per adempiere alle predette prescrizioni e per conseguire il migliore livello di protezione dei dati personali trattati dal titolare del trattamento, sono adottate le misure di sicurezza illustrate nei paragrafi che seguono.

Nell'ambito dell'organizzazione del lavoro, ai soli fini degli adempimenti di legge, i dati personali oggetto di trattamento vengono divisi in relazione alla loro natura in due principali classi:

1. Dati personali ordinari (comuni), di tipo generico, e comprende i dati relativi ai dipendenti, clienti, consulenti, fornitori, ecc. relative alle persone fisiche;
2. Dati personali particolari e giudiziari, (si vedano le definizioni sopra esposte).

Si dispone, comunque che, i trattamenti relativi ai dati delle procedure ed operazioni finalizzate agli adempimenti:

- Di legge;
- Del sistema dei controlli interni;
- Richiesti da parte della Magistratura e delle Autorità Finanziarie;

siano protetti con le misure di sicurezza previste per i dati anche particolari e giudiziari.

5 AUTORIZZATI DEL TRATTAMENTO

Ad integrazione delle disposizioni emanate in precedenza dall'Ente, si conferma che ai sensi dell'art. 32 comma quarto, del Regolamento UE, il personale dipendente in servizio presso l'Ente è autorizzato a trattare i dati personali necessari per lo svolgimento delle attività e delle funzioni ad esso collettivamente affidate e di compiere le operazioni di trattamento a ciò strumentali, attenendosi anche alle ulteriori istruzioni contenute nel presente regolamento, o impartite nel corso dell'attività e rispettando le pertinenti disposizioni contenute in specifiche comunicazioni interne indirizzate alle categorie di autorizzati interessati.

Gli autorizzati, appositamente nominati, di norma, possono trattare i soli dati inerenti alle attività del settore organizzativo a cui sono assegnati e non devono eseguire operazioni di trattamento per finalità non previste dall' Ente.

Tra gli autorizzati sono stati compresi i consulenti con contratto di collaborazione, anche se per attività occasionali limitatamente al periodo necessario ed ai soli trattamenti pertinenti l'attività da svolgere.

Alcune tipologie di dati (es. particolari, giudiziari o che presentano rischi specifici) possono essere trattate esclusivamente dalle categorie di autorizzati di seguito specificate ivi compresi i diretti superiori degli autorizzati stessi.

5.1 ISTRUZIONI GENERALI PER TUTTI I DIPENDENTI E GLI AUTORIZZATI

Gli autorizzati, nel trattare i dati personali, dovranno operare garantendo la massima riservatezza ed integrità delle informazioni di cui vengono in possesso.

In particolare il dipendente, nell'ambito del suo rapporto di lavoro pubblico, rispetta il segreto d'ufficio nei casi e nei modi previsti dalle norme dell'ordinamento e un particolare dall'art. 24 della legge n. 241/1990 e mantiene riservate le notizie e le informazioni apprese nell'esercizio delle proprie funzioni e che non siano oggetto di trasparenza in conformità alla legge e ai regolamenti. Il dipendente osserva il dovere di riservatezza anche dopo la cessazione dal servizio.

In particolare, il dipendente non fornisce informazioni in merito ad attività istruttorie, ispettive o di indagine in corso presso l'Ufficio e non rilascia informazioni relative ad atti e provvedimenti prima della loro comunicazione alle parti.

Il dipendente non fa uso delle informazioni non disponibili al pubblico o non rese pubbliche, ottenute anche in via confidenziale nell'attività d'ufficio, a fini privati e deve evitare situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine dell'Ente.

L'autorizzato al trattamento deve osservare scrupolosamente le disposizioni che regolano l'accesso ai locali dell'amministrazione da parte del personale e non introdurre, salvo che non siano debitamente autorizzate, persone estranee all'Ente stesso in locali non aperti al pubblico.

Gli autorizzati dovranno perciò operare con la massima diligenza ed attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento, così per la conservazione ed eventuale cancellazione o distruzione.

La procedura di lavoro e la condotta tenuta nello svolgimento delle operazioni di trattamento, dovranno essere orientate a prevenire i rischi che potrebbero incombere sui dati, in particolare evitando che:

- i dati personali siano soggetti a distruzione e perdita anche accidentale,
- ai dati possano accedere persone non autorizzate,
- vengano svolte operazioni di trattamento non consentite,
- vengano svolte operazioni per fini diverse da quelli per i quali i dati sono stati raccolti.

Taluni autorizzati di trattamenti di dati particolari e giudiziari sono destinatari di ulteriori specifiche indicazioni che integrano quelle generali di cui al presente regolamento. Le ulteriori disposizioni sono indicate nei singoli atti di nomina.

5.2 LISTA DEGLI AUTORIZZATI ED AGGIORNAMENTO NELL'AMBITO DEL TRATTAMENTO

Il Titolare del Trattamento del dato e qualsiasi altra funzione delegata, conserva la lista degli autorizzati, comprendente l'ambito del trattamento riservato a ciascun autorizzato e la natura dei dati trattati dallo stesso (dati comuni, particolari, giudiziari), aggiornata e verificata periodicamente (comunque almeno una volta l'anno) dal responsabile dell'Area Tecnologica (IT) o dall'amministratore di sistema.

La lista degli autorizzati e l'ambito del trattamento consentito è correlata ai singoli profili di accesso alle reti informatiche operative aggiornate seguendo il principio che gli autorizzati hanno accesso ai soli dati necessari per lo svolgimento delle loro attività.
I profili di accesso assegnati ai singoli autorizzati sono registrati e conservati in un database informatico costantemente aggiornato e disponibile in caso di verifiche.

5.3 ESCLUSIONI DALLE OPERAZIONI DI TRATTAMENTO

Gli addetti alla manutenzione di strumenti elettronici e qualsiasi altro addetto appartenente ad altre ditte che per necessità operative accedono agli uffici dell'Ente (es. addetto alle pulizie) non sono autorizzati a svolgere nessuna operazione di trattamento. Gli autorizzati adottano i comportamenti adatti ed adeguati ad evitare che ai trattamenti da loro svolti accedano, pur se accidentalmente, le persone non autorizzate.

6 VERIFICHE E CONTROLLI PERIODICI

Ai sensi dell'art. 32, primo comma, lettera d) del Regolamento UE sono previste verifiche e controlli periodici circa la puntuale osservanza delle disposizioni di cui al presente Regolamento.

7 NORME PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI

La presente sezione del Regolamento comprende le istruzioni operative generali relative ai trattamenti svolti con strumenti elettronici secondo quanto previsto dal Manuale di procedura/Lista delle misure di sicurezza:

- ***Sistema di autenticazione informatica;***
- ***Misure di Sicurezza***
  - Antivirus e protezione da programmi pericolosi;
  - Protezione dalle intrusioni e dagli accessi abusivi;
  - Memorizzazione dei log di sistema
  - Procedure di aggiornamento dei programmi per elaboratore per prevenire vulnerabilità e correggere difetti;
  - Procedura per la custodia di copie di sicurezza;
  - PC portatili
  - Licenze d'uso dei programmi software
  - Internet e posta elettronica
  - Smartphone
  - Conversazioni telefoniche
  - Conversazioni Vivavoce
  - Fax
  - Autorizzazioni all'ingresso nei locali e controllo accesso ai locali.
  - Cifratura
  - Custodia e riutilizzo dei supporti;
  - Ripristino dell'accesso ai dati

7.1 SISTEMA DI AUTENTICAZIONE INFORMATICA

7.1.1 AUTENTICAZIONE INFORMATICA

Le credenziali di autenticazione, consistono in un sistema per l'identificazione dell'autorizzato (User-ID / login / user name / utente) associato ad una parola chiave (Password / parola d'ordine) riservata, conosciuta solamente dal medesimo.

7.1.2 PROCEDURA DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Ad ogni autorizzato possono essere assegnate o associate più credenziali di autenticazione per l'accesso a sistemi diversi.

Le credenziali assegnate agli autorizzati possono essere: le parole chiave, i codici per l'accesso, eventuali certificati digitali, le smart card, i token per la generazione automatica di codici, ecc..

Si informa che in caso di non utilizzo delle credenziali per un periodo di 6 mesi o in caso di perdita della qualità che consente all'autorizzato l'accesso ai dati personali, in ottemperanza alle disposizioni di legge, le stesse credenziali sono disattivate.

La disattivazione delle credenziali non riguarda le credenziali preventivamente autorizzate ed assegnate per finalità di gestione tecnica e di emergenza dei sistemi, fermo restando la loro custodia sicura. Di seguito sono indicati i criteri e le modalità per la custodia.

Parola chiave per l'accesso ai dati

Gli "autorizzati" possono accedere alla rete o ai sistemi di file sharing utilizzati e quindi alle attività di trattamento dei dati, solo utilizzando, oltre al codice identificativo, una **parola chiave** personale.
Nell'utilizzo delle parole chiave, ogni "autorizzato" deve attenersi, anche, alle seguenti norme di sicurezza:

- al momento dell'inserimento in una unità organizzativa dell'Ente e/o alla presa in carico di un personal computer, deve sostituire immediatamente la parola chiave iniziale/transitoria comunicata, con una parola chiave personale secondo le specifiche sotto indicate;
- non deve divulgare la parola chiave personale o comunicarla o trasmetterla ad altri, possibilmente non deve conservarla scritta e comunque deve evitare che sia conosciuta, anche accidentalmente, da altre persone;
- deve sostituire la parola chiave, in modo autonomo, con cadenza almeno semestrale o quando ritenga che, per qualunque motivo, abbia perso le caratteristiche di segretezza.

I personal computer quando sono dati in carico agli autorizzati, per assunzioni o trasferimenti di mansioni, sono abilitati con una parola chiave "scaduta", ovvero che viene disattivata subito dopo la prima attivazione.

La parola chiave "password" viene scelta liberamente dai singoli autorizzati, ma per garantirne l'affidabilità, deve avere le seguenti caratteristiche definite nei requisiti minimi di complessità definiti dall'Ente

- utilizzo misto di caratteri numerici e alfabetici, possibilmente non a scansione fissa scegliendo tra maiuscole e minuscole;
- non utilizzo contemporaneo o ripetitivo di password uguali o complementari o frazionate.

La parola chiave, con il codice identificativo, deve essere il solo mezzo per attivare il proprio personal computer.

Codice identificativo personale

Il **Codice Identificativo personale** (user identification) per l'accesso alla rete e/o ai sistemi di file sharing è personale ed univoco.
Lo stesso Codice Identificativo Personale non potrà essere attribuito, nemmeno in tempi diversi, a persone diverse.
Salvo casi eccezionali, con lo stesso Codice Identificativo Personale, non si possono attivare o utilizzare più personal computer contemporaneamente.
In caso di dimissioni il Codice Identificativo Personale del dimissionario viene reso inutilizzabile.
In caso di non utilizzo del Codice Identificativo Personale per un periodo consecutivo di sei mesi, il Codice Identificativo Personale viene disattivato.

7.1.3 PROTEZIONE DELLA SESSIONE DI TRATTAMENTO

È fatto obbligo di non lasciare incustodito ed accessibile lo strumento elettronico (generalmente il personal computer) durante una sessione di trattamento. Allo scopo gli autorizzati nel caso di abbandono temporaneo della postazione di lavoro, proteggono la sessione di lavoro adottando una delle seguenti misure:

- premere contemporaneamente i tasti Ctrl + Alt + Canc e quindi INVIO oppure tramite il tasto di scelta rapida "Logo Windows" + L ;
- effettuare un "log off" della stazione di lavoro utilizzata; (tale operazione è comunque fatta al termine delle attività salvo diversi accordi).

7.1.4 DISPOSIZIONI PER ASSICURARE LA DISPONIBILITÀ DI DATI O STRUMENTI ELETTRONICI IN CASO DI ASSENZA O IMPEDIMENTO DELL'AUTORIZZATO

In caso di assenza o impedimento dell'autorizzato, l'Ente potrebbe trovarsi nella circostanza di dover accedere allo strumento o ai dati trattati dalla persona assente. Per tali motivi le parole chiave, autonomamente sostituite da ciascun autorizzato, sono conservate e custodite nel rispetto delle modalità di conservazione informatica.

La modalità di custodia informatica - che riguarda la totalità degli Autorizzati - prevede che tutte le parole chiave per l'accesso alla rete siano create, registrate e gestire su database del sistema di autorizzazione informatico adottato dall'Ente, accessibile attraverso il relativo meccanismo di sicurezza.

Ove per ragioni organizzative sia necessaria la conoscenza della parola chiave, l'amministratore di sistema provvederà al reset della password per poter accedere ai dati ed alle attività in rete di un autorizzato.

Questa procedura dovrà essere supervisionata da un responsabile che ne avrà autorizzato l'esecuzione e che darà immediata notizia all'autorizzato al suo rientro;

7.2 SISTEMA DI AUTORIZZAZIONE

L'ambito dei trattamenti previsti per ciascun autorizzato è correlato ai compiti ed alle funzioni svolte nell'unità organizzativa di assegnazione. Questi trattamenti possono dar luogo all'assegnazione di un profilo di autorizzazione.
Tali profili sono organizzati per classi omogenee di comportamento e configurati anteriormente all'inizio del trattamento in maniera tale da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento nell'ambito assegnato all'autorizzato. Annualmente deve essere verificato che i soggetti che accedono ai dati abbiano conservato le stesse qualità che consentono l'accesso.

7.2.1 AUTORIZZAZIONI AGLI ADDETTI DELLA MANUTENZIONE

I soggetti addetti alla manutenzione delle apparecchiature della rete sono autorizzati a svolgere le operazioni di manutenzione senza accedere ai dati e salvaguardandoli da distruzione o cancellazione casuale.

Nel caso la manutenzione si riferisca a guasti e non ad aggiornamenti del software, ed in particolare nel caso si renda necessario la rimozione di dischi o supporti magnetici per essere trasportati in laboratori esterni, il tecnico di manutenzione dovrà essere nominato provvisoriamente "Autorizzato".

7.3 Misure di sicurezza

7.3.1 ANTIVIRUS E PROTEZIONE DA PROGRAMMI PERICOLOSI

L'uso di programmi antivirus è obbligatorio per tutti i personal computer collegati, anche temporaneamente in rete.
Tutti i personal computer, collegati alla rete e/o ai sistemi di file sharing, sono controllati in modo automatico da un software antivirus gestito centralmente e aggiornato costantemente che, di norma, viene attivato all'accensione del computer e rimane residente in memoria fino allo spegnimento dello stesso.
Tutti gli autorizzati devono controllare che l'operazione di verifica con i programmi antivirus sia correttamente e completamente eseguita, segnalando qualsiasi anomalia e, in tal caso, spegnendo il proprio personal computer.
Tutti gli autorizzati che devono trattare, anche solo in lettura, supporti che non siano già stati testati, devono controllare gli stessi con il programma antivirus.
Ciascun autorizzato che riceva programmi e/o dati da destinatari esterni all'ente deve controllarli (con antivirus) prima di attivarli o aprirli.

7.3.2 PROTEZIONE DALLE INTRUSIONI E DAGLI ACCESSI ABUSIVI

I servizi di collegamento ad Internet e di posta elettronica sono gestiti e protetti nell'architettura globale del sistema informatico dell'Ente. L'accesso alla rete pubblica (internet), effettuato con tali servizi, è protetto da sistemi attivi e da apposito dispositivo detto "firewall" in cui sono attivi servizi di protezione che sono costantemente aggiornati.

Alcuni di questi servizi permettono:

- individuazione delle attività dannose e di registrarne le informazioni tentando di bloccarle e segnalarle (IPS)
- può limitare l'uso di applicazioni improduttive, inappropriate e pericolose
- controlla l'attività web
- protezione in tempo reale, continua e affidabile contro spam e tentativi di phishing
- prevenzione dalla violazione dei dati (DLS)
- difesa contro malware (TDR e APT blocker)

La rete Wi-Fi è disponibile sia agli operatori dell'Ente che ai visitatori esterni e permette l'esclusivo accesso alla rete pubblica (internet). Anche tale rete è protetta dal sistema di protezione perimetrale dell'Ente sopra definito (*"firewall"*).

7.3.3 MEMORIZZAZIONE DEI LOG DI SISTEMA

Tutti i dispositivi, o quasi, ormai sono in grado di generare dei log e di memorizzarli localmente o su un server di log.

La memorizzazione dei log per un determinato periodo di tempo è necessaria per poter consultare in caso di una violazione di dati e per avere degli avvertimenti in caso comportamenti anomali rispetto alla normale attività.

7.3.4 PROCEDURE DI AGGIORNAMENTO DEI PROGRAMMI PER ELABORATORE PER PREVENIRE VULNERABILITÀ E CORREGGERE DIFETTI

I gestori del sistema curano l'aggiornamento periodico, finalizzato alla prevenzione delle vulnerabilità e alla correzione dei difetti, dei programmi e dei sistemi sulla base dei rilasci effettuati dai fornitori (software-house). La periodicità di tale aggiornamento è almeno semestrale e per i trattamenti di dati particolari o giudiziari trimestrale.

Sono attivi sui personal computer, con sistema operativo Windows, aggiornamenti periodici automatizzati al fine di prevenire vulnerabilità e correggere difetti.

7.3.5 PROCEDURA PER LA CUSTODIA DI COPIE DI SICUREZZA

Si provvede alla generazione delle copie di sicurezza (backup) dei dati trattati dall'Ente secondo gli standard stabiliti, avendo cura della conservazione in sicurezza delle copie di backup su supporti rimovibili e in cloud. La frequenza delle copie è giornaliera, anche su dispositivi diversi e con modalità diverse.

7.3.6 PC PORTATILI

In caso di assegnazione di PC portatili, devono essere adottate le seguenti misure di sicurezza oltre alle misure di sicurezza sopra descritte.
Premesso che non è consentita di norma la memorizzazione di dati personali, qualora ciò sia indispensabile per fini connessi alle attività lavorative svolte:

- Il computer dovrà essere protetto anche con una parola chiave all'accensione dello strumento (password di BIOS);
- La lunghezza dovrà essere pari al numero di posizioni rese disponibili dalla funzione (cioè tutte le caselle).

La password di BIOS sarà assegnata dall'amministratore di sistema in accordo con il responsabile delle Unità Organizzative e dovrà essere conservata secondo la procedura già in atto per le password.

Ove necessario periodicamente l'amministratore di sistema con il responsabile delle Unità Organizzative provvede alla sostituzione della password di BIOS comunicandola all'utente autorizzato all'uso.
L'aggiornamento del software antivirus e dei programmi per elaboratore, finalizzato alla prevenzione delle vulnerabilità e alla correzione dei difetti, viene effettuato automaticamente all'atto del collegamento alla LAN. Si raccomanda agli assegnatari di PC portatili di effettuare periodicamente il collegamento alla rete e/o ai sistemi di file sharing per garantire l'aggiornamento dei prodotti. I dati trattati dall' Ente eventualmente contenuti sui PC portatili, nel caso non

siano già stati registrati su sistema centrale o su dischi rete o dipartimentali, con cadenza periodica almeno settimanale, devono essere trasferiti sul disco di rete assegnato allo scopo di evitarne la perdita anche se accidentale.
Per tutti i dispositivi portatili considerati ad uso comune (per esempio pc sala congressi/conferenze enpam) la password di BIOS non ha senso dovrebbe essere comunicata a troppe persone ad ogni modo questi dispositivi verrà predisposta un utente per autenticazione comune la cui password sarà variata regolarmente almeno ogni due mesi.

Questi portatili con le autenticazioni assegnate a uso comune non potranno accedere alla rete LAN dell'ordine ma avranno accesso solo alla navigazione internet.

7.3.7 LICENZE D'USO DEI PROGRAMMI SOFTWARE

E' fatto divieto, per la normativa sul diritto di autore, di copiare, installare o utilizzare programmi software non rilasciati ufficialmente dall'Ente e preventivamente testati circa la loro liceità, integrità e compatibilità con gli standard dell'Ente.

Pertanto ogni necessità di installazione di prodotti cosiddetti "in demo" o "trial", potrà essere installata previa verifica con l'amministrazione di sistema.

7.3.8 INTERNET E POSTA ELETTRONICA

La connessione ad internet deve avvenire per finalità professionali.

L'eventuale acquisto di programmi via internet, potrà essere effettuato esclusivamente da persone appositamente autorizzate dall'Ente.

Non è consentito l'uso di internet per la ricezione di programmi radio e musicali, e conversazioni in chat line o collegamenti a webcam, salvo per motivi professionali.

Le caselle di posta elettronica sono messe a disposizione dall'Ente per usi esclusivamente professionali, l'improprio uso personale, comporta assunzione diretta di responsabilità circa i contenuti dei messaggi da parte di chi li invia. La casella di posta deve essere mantenuta in ordine, cancellando documenti. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoghe diciture, deve essere visionata od autorizzata dal responsabile dell'ufficio, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria. È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile del trattamento. Non si devono in alcun caso attivare gli allegati di tali messaggi.

7.3.9 CONVERSAZIONI TELEFONICHE

Non è consentito fornire informazioni riservate sugli iscritti ed altri enti che intrattengono rapporti con l'Ente, o sulle attività svolte dall'Ente stessa ovvero sul proprio personale, se non si è certi di chi sia l'interlocutore e, comunque, al di fuori dell'ambiente di lavoro, senza autorizzazione.

Spie industriali, pirati informatici (hacker) e altre persone che vogliono accedere ai sistemi dell'Ente spesso si camuffano per venire a conoscenza di numeri telefonici interni, password, nomi di collaboratori, ecc. A questa pratica viene dato il nome di "social engineering". Tutte le informazioni, anche se in apparenza irrilevanti, possono essere usate per organizzare un attacco informatico ai sistemi della Ente.

È fatto divieto, quindi, di fornire telefonicamente informazioni sull'organizzazione interna e/o codici identificativi, password, assenze a sconosciuti.

Nell'effettuare una telefonata riguardante la propria attività, assicurarsi che la persona contattata sia esattamente quella desiderata ed evitare il rischio che persone estranee possano volontariamente o involontariamente ascoltare il contenuto della telefonata.

7.3.10 SMARTPHONE

L'Ente non dispone di smartphone ad uso interno ed è vietato l'uso dei personali per svolgere compiti istituzionali.

Tutti gli smartphone personali devono essere collegati alla WIFI esterna per la sola connettività internet.

7.3.11 CONVERSAZIONI VIVA VOCE

Nel caso la conversazione telefonica venga svolta in modalità "viva voce" (ad esempio durante le "conference call"), l'interlocutore dovrà essere informato circa l'eventuale presenza di altri ascoltatori. Inoltre, in caso di conversazioni riservate, assicurarsi che tutti gli interlocutori siano informati della riservatezza della comunicazione.

7.3.12 FAX

Evitare l'invio di messaggi fax inutili. Usare la dovuta cautela nell'invio informale di messaggi fax, il loro contenuto potrebbe essere considerato come una formale comunicazione della Ente. Nell'invio di un fax contenente dati personali ad una persona autorizzata a visionarli, assicurarsi che il documento non capiti nelle mani di persone non autorizzate a conoscere tali informazioni, sia presso il mittente che presso il destinatario, invitando, la persona destinataria ad essere vicina all'apparecchiatura ricevente al momento della spedizione/ricevimento.

In ogni caso, per la trasmissione di informazioni via fax, si ricorda a tutto il personale di adottare i template dell'Ente messi a disposizione.

7.3.13 AUTORIZZAZIONI ALL'INGRESSO NEI LOCALI E CONTROLLO ACCESSO AI LOCALI

L'ingresso nei locali dove sono presenti le apparecchiature di gestione della rete dell'Ente dei personal computer e nei locali dove sono presenti le apparecchiature di gestione del sistema informativo dell'Ente (Server) è riservato alle seguenti persone autorizzate:

Sig. Michela Bonet
Sig. Alessio Ciciliani
Sig. Massimo Amoruso (amministratore di sistema).

7.3.14 CIFRATURA

Per tutti i dispositivi in cui è possibile attiva la cifratura a livello di volume questa deve essere attiva, mentre per i trattamenti si predispongono dei contenitori cifrati sono per dati particolari.

7.3.15 CUSTODIA E RIUTILIZZO DEI SUPPORTI RIMOVIBILI

Gli autorizzati, ai quali è stato permesso il trattamento del dato tramite l'utilizzo di supporti rimovibili, debbono custodirli e controllarli in modo tale che soggetti non autorizzati non possano venire a conoscenza, nemmeno accidentalmente, del contenuto di tali supporti. I supporti devono essere protetti da cifratura e al termine di ogni lavorazione dovranno essere custoditi e riposti in contenitori, armadi o cassetti muniti di serratura.

In caso di cattivo funzionamento del supporto, che ne determini l'impossibilità della lettura dei dati registrati, i supporti dovranno essere distrutti.

Nel caso di supporti contenenti dati personali, si precisa che la formattazione di un disco o di una "*chiavetta USB*" non costituisce norma di sicurezza poiché i dati formattati possono essere recuperati e letti attraverso apposite "utility"; pertanto i supporti devono essere trattati per permettere una distruzione completa e definitiva del dato in esso contenuto, arrivando in taluni casi anche alla distruzione materiale del supporto (ad es. i DVD).

7.3.16 RIPRISTINO DELL'ACCESSO AI DATI

In caso di danneggiamenti che dovessero interessare dati particolari e giudiziari ovvero gli strumenti che li contengono, i gestori del sistema, assicurano il ripristino dell'accesso a tali dati (della loro disponibilità ed integrità) in tempi certi compatibili con le esigenze di utilizzo degli utenti interessati e comunque non superiori ai sette giorni.

8 NORME PER I TRATTAMENTI SVOLTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Nel caso di trattamenti di dati personali senza l'ausilio di strumenti elettronici, e quindi con modalità essenzialmente manuali e cartacee, il presente Regolamento descrive le misure di sicurezza che debbono essere osservate.

Vengono a tale proposito adottate all'interno dell'Ente le seguenti misure organizzative e procedurali, che oltre ad adempiere ai livelli minimi previsti dalla legge, hanno l'obiettivo di assicurare una migliore e più ampia tutela dei documenti e dei dati personali in essi contenuti.

La presente sezione di regolamento comprende le istruzioni operative generali relative a:

- ***Custodia e controllo di atti e documenti***
  - Accesso ai soli dati necessari
  - Restituzione atti e documenti al termine delle operazioni
- ***Accesso controllato agli archivi***
  - Identificazione e registrazione dei soggetti ammessi agli archivi dopo l'orario di chiusura
- ***Ulteriori misure di sicurezza***
  - Custodia e conservazione delle riproduzioni
  - Distruzione di documenti cartacei

8.1 CUSTODIA E CONTROLLO DI ATTI E DOCUMENTI

La consultazione di materiale di archivio è considerata trattamento di dati, quindi soggetta ad idonee e preventive misure di sicurezza.

Gli autorizzati del trattamento devono conservare e custodire i dati trattati con la massima riservatezza evitando che vengano volontariamente o involontariamente conosciuti da soggetti non dipendenti dell'Ente.

L'accesso agli archivi contenenti atti e documenti di dati personali di qualunque natura (ordinari, particolari e giudiziari o che presentano specifiche rischiosità) è riservato alle sole persone incaricate ed autorizzate a potervi accedere con apposita nomina.

Sono autorizzate ad accedere agli archivi tutte le persone che operano con la qualificazione di autorizzato (dipendenti, consiglieri e collaboratori autorizzati) nei limiti previsti dalla nomina stessa.

Gli atti e i documenti cartacei contenenti dati personali di qualunque natura (comuni, particolari o giudiziari), devono essere trattati con diligenza, custoditi e conservati in maniera che le persone non incaricate non possano venirne a conoscenza - con particolare riguardo a quelli particolari e giudiziari.

L'autorizzato consulta i soli atti e fascicoli ai quali è autorizzato ad accedere e ne fa un uso conforme ai doveri d'ufficio e alla mansione, consentendone l'accesso a coloro che ne abbiano titolo e in conformità alle prescrizioni impartite dall'Ente. Previene inoltre, l'eventuale dispersione di dati osservando le misure di sicurezza impartite, custodendo con ordine e cura gli atti affidati ed evitando di effettuarne inutili copie.

Durante l'utilizzazione i documenti, ed i fascicoli cartacei, non devono essere lasciati incustoditi.

In caso di trattamenti di dati particolari è prestata la massima attenzione affinché tali dati non siano conosciuti da persone prive della qualificazione di autorizzato o che pur avendo la qualifica non siano autorizzati al trattamento di tali dati.

L'autorizzato al trattamento di dati particolari provvede a chiudere gli archivi contenenti tali dati alla fine della giornata lavorativa.

I documenti (o copia degli stessi) contenenti dati particolari non possono essere, senza specifica autorizzazione, asportati dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati. In caso di assenza temporanea durante l'utilizzo i documenti vanno riposti nei cassetti o armadietti a sua disposizione o chiusi negli uffici per evitare che possano essere effettuati trattamenti da soggetti non autorizzati.

Per l'acceso ai dati al di fuori del normale orario di lavoro dovrà essere chiesta specifica autorizzazione.

8.1.1 ACCESSO AI SOLI DATI NECESSARI

Durante lo svolgimento di trattamenti di dati personali ordinari, registrati, stampati o riprodotti su carta o altri supporti non informatici, i singoli autorizzati delle diverse operazioni di trattamento devono operare in maniera da svolgere le operazioni di trattamento solo su quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti per le specifiche attività attribuite alla funzione ricoperta. È pertanto vietata ogni forma di trattamento di dati personali non pertinente con le finalità lavorative.

8.1.2 RESTITUZIONE ATTI E DOCUMENTI AL TERMINE DELLE OPERAZIONI

Gli atti e i documenti cartacei devono essere trattenuti presso la propria postazione di lavoro (scrivania) solo per il periodo strettamente necessario allo svolgimento delle operazioni necessarie. Al termine delle operazioni svolte devono essere riposti negli archivi o nei contenitori dedicati.

8.2 ACCESSO CONTROLLATO AGLI ARCHIVI

L' Ente dispone di archivi attivi. Gli archivi attivi sono costituiti dagli armadi di stanza. Alcuni armadi e le cassettiere di scrivania sono dotate di serratura. L'accesso è consentito solo al personale che ne gestisce il contenuto.

8.2.1 IDENTIFICAZIONE E REGISTRAZIONE DEI SOGGETTI AMMESSI AGLI ARCHIVI DOPO L'ORARIO DI CHIUSURA

Le persone che accedono ai locali ove sono situati gli archivi contenenti atti e documenti di dati particolari e giudiziari dopo l'orario di chiusura, devono essere preventivamente identificate ed autorizzate.

8.3 ULTERIORI MISURE DI SICUREZZA

8.3.1 CUSTODIA, ARCHIVIAZIONE E CONSERVAZIONE DELLE RIPRODUZIONI

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi si è provveduto ad istruire gli autorizzati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti, soprattutto quelli di natura particolare e di tenere ordine e pulizia nelle proprie scrivanie e uffici.

Vengono date disposizioni di accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati; in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore o ad un responsabile del trattamento o direttamente al Titolare.

Di conseguenza, agli autorizzati, è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative; tali documenti, devono essere controllati e custoditi, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi essere restituiti all'archivio, al termine di tale ciclo.

Gli autorizzati custodiscono in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative. A tale fine, il personale è stato dotato ove possibile di:

- cassetti con serratura,
- armadi chiudibili a chiave,
- cassaforte.

In tali attrezzature si devono riporre i documenti contenti i dati prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli nei giorni successivi. Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti non più necessari per lo svolgimento delle proprie mansioni lavorative. Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni

I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali particolari e giudiziari ovvero di dati personali della Ente devono essere custoditi e conservati con le stesse modalità previste dal regolamento nei punti precedenti, per i trattamenti degli atti e dei documenti originali.

8.3.2 DISTRUZIONE DI DOCUMENTI CARTACEI

Nel caso di destinazione a macero di documenti contenenti dati personali di qualsiasi natura, sia comuni sia di tipo particolari e giudiziario, l'Autorizzato deve curare che i dati in questione non possano venire a conoscenza di persone che non abbiano la stessa qualifica di Autorizzato (come il personale esterno addetto alle operazioni di macero) predisponendoli in maniera opportuna.

Pertanto, prima dell'avvio al macero, i documenti costituiti da fogli singoli, ovvero da un numero di pagine contenuto, andranno distrutti singolarmente mentre i documenti con maggior numero di pagine, ovvero i tabulati risultanti da trattamenti automatizzati, dovranno essere confezionati (riposti in scatoloni chiusi con nastro adesivo e con l'indicazione all'esterno dello scatolone di "macero riservato") in maniera da garantirne la riservatezza per il successivo processo di macero effettuato dal personale addetto a tale incombenza.

Luogo e data,

TITOLARE DEL TRATTAMENTO
Timbro e firma Presidente dell'Ordine