LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

PREMESSA 2
1 INFORMAZIONI GENERALI SULLA PROTEZIONE DEI DATI PERSONALI 3
2 PRINCIPALI CONCETTI E DEFINIZIONI 4
3 AUTORIZZATI DEL TRATTAMENTO 5
3.1 ISTRUZIONI GENERALI PER TUTTI GLI AUTORIZZATI 6
4 USO DEGLI STRUMENTI E RELATIVE ISTRUZIONI 6
4.1 REGOLE PER LA GESTIONE DELLE PASSWORD 6
4.2 DISPONIBILITÀ DI DATI O STRUMENTI ELETTRONICI IN CASO DI ASSENZA 7
4.3 PROTEZIONE DELLA SESSIONE DI TRATTAMENTO 7
4.4 MISURE DI SICUREZZA 8
4.4.1 ANTIVIRUS E PROTEZIONE DA PROGRAMMI PERICOLOSI 8
4.4.2 PROTEZIONE DALLE INTRUSIONI E DAGLI ACCESSI ABUSIVI 8
4.4.3 MEMORIZZAZIONE DEI LOG DI SISTEMA 9
4.4.4 PROCEDURE DI AGGIORNAMENTO DEI PROGRAMMI PER ELABORATORE PER PREVENIRE VULNERABILITÀ E CORREGGERE DIFETTI 9
4.4.5 PROCEDURA PER LA CUSTODIA DI COPIE DI SICUREZZA 9
4.4.6 PC PORTATILI 9
4.4.7 LICENZE D'USO DEI PROGRAMMI SOFTWARE 10
4.4.8 INTERNET E POSTA ELETTRONICA 10
4.4.9 CONVERSAZIONI TELEFONICHE 11
4.4.10 AUTORIZZAZIONI ALL'INGRESSO NEI LOCALI E CONTROLLO ACCESSO 11
4.4.11 CIFRATURA 11
4.4.12 CUSTODIA E RIUTILIZZO DEI SUPPORTI RIMOVIBILI 11
4.4.13 USO STAMPANTI 12
4.4.14 CLOUD COMPUTING 12
5 ARCHIVI CARTACEI 12
6 DISPOSIZIONI FINALI 13

LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

PREMESSA

Le presenti Linee Guida sono emanate dall'Ordine dei Medici Chirurghi e degli Odontoiatri di Padova (" di seguito denominato Ente") 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 completano ogni altra procedura interna dell'Ente a protezione dei dati personali, con particolare riferimento alle misure di sicurezza poste a tutela dei trattamenti effettuati con strumenti elettronici di qualunque natura e tipologia a tutela dei dati personali disposti in archivi informatici dell'Ente o di fornitori terzi di servizi in cloud.

L'Ente nell'espletamento della sua attività istituzionale opera prestando attenzione alla sicurezza delle informazioni e dei dati, perseguendo adeguati livelli di sicurezza del proprio sistema informativo e adottando idonee misure organizzative e tecnologiche, volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia per proteggere i dati personali detenuti, sia per difendere tutte le informazioni presenti nelle banche dati informatiche (di seguito denominati "Database").

A chi si rivolge questo documento e la portata dello stesso

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici, da parte dei dipendenti e dei componenti gli Organi Istituzionali e Commissioni dell'Ente e per quanto compatibili a tutti coloro che, in virtù di un incarico qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, etc.), utilizzano o forniscono strumenti informatici o servizi in favore dell'Ente ("Destinatari").

Le presenti linee guida integrano il Codice di Comportamento comportamentale dell'Ente emanato con Deliberazione N° 14 del 16.01.2024 e sono inserite in una sezione dedicata dello stesso, ai sensi ai sensi dell'art. 54 co. 1 bis del D.Lgs. 30 marzo 2001 n. 165.

Scopo di questo documento è anche quello di essere un valido supporto alle funzioni e alle attribuzioni della funzione di Responsabile della Transizione Digitale dell'Ente il quale deve operare in piena autonomia col supporto del Responsabile della protezione dei dati ("DPO") e dell'Amministratore di sistema ("ADS").

Tali prescrizioni integrano le specifiche istruzioni fornite a tutti gli Autorizzati art. 29 Regolamento UE, in attuazione della normativa in materia di protezione dei dati personali.

Le informazioni contenute nelle presenti Linee Guida vengono rilasciate, pera quanto compatibili, anche ai sensi dell'art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata a tutti i soggetti interessati e dell'art. 4 dello Statuto dei Lavoratori Legge n. 300/1970.

Finalità del documento

Il presente documento definisce e detta ai Destinatari specifiche regole di comportamento e condizioni di utilizzo degli strumenti informatici attraverso:

- la definizione di regole e procedure uniformi da applicarsi all'interno dell'Ente;
- l'osservanza dei doveri minimi di diligenza, lealtà, imparzialità e buona condotta;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;

- definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili nel rispetto della normativa vigente;
- individuazione delle responsabilità dei Destinatari in caso di inosservanza di regole e prescrizioni.

Fonti

Le presenti Linee Guida e sono redatte in conformità alle seguenti fonti normative, regolamentari, linee guida e strumenti di soft law:

- Codice di comportamento dei dipendenti pubblici approvato con DPR 16 aprile2013 n. 62;
- Provvedimento del Garante per la protezione dei dati personali (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007);
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella GU n. 300 del 24 dicembre 2008;
- Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (GDPR) e il Codice Privacy D. Lgs. 196/2003 armonizzato;
- Piani Triennali per l'informatica della PA;
- Standard ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti).

1 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.

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.

LINEE GUIDA SUL CORRETTO UTILIZZO DELLE TECNOLOGIE INFORMATICHE E DEGLI ARCHIVI

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

2 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.

"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.

"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. 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.

"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.

"RESPONSABILE PROTEZIONE DATI" o data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento europeo, è un professionista con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

"**AMMINISTRATORE DI SISTEMA"** soggetto designato a sovraintendere il funzionamento del sistema informatico dell'Ente. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, che deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. La designazione quale amministratore di sistema è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni loro attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante per la Protezione dei Dati Personali. L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di verifica da parte dell'Ente, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

3 AUTORIZZATI DEL TRATTAMENTO

Ai sensi dell'art. 32 comma quarto, e dell'art. 29 del Regolamento UE, il personale dipendente in servizio presso l'Ente nonché tutti i componenti gli Organi Istituzionali e delle Commissioni e i collaboratori a vario titolo (es. stagisti o somministrati) sono nominati con apposito atto scritto, autorizzati a trattare i dati personali necessari per lo svolgimento delle attività e delle funzioni ad essi affidate in funzione del proprio incarico e di compiere le operazioni di trattamento a ciò strumentali, attenendosi anche alle ulteriori istruzioni contenute nel presente documento, o impartite nel corso dell'attività e rispettando le pertinenti disposizioni contenute in specifiche comunicazioni interne indirizzate alle categorie di autorizzati interessati.

Gli autorizzati 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.

L'Ente 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) con il supporto responsabile della protezione dei dati (DPO) e dell'amministratore di sistema (ADS), il quale aggiorna i singoli profili di accesso alle reti informatiche 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.

3.1 ISTRUZIONI GENERALI PER TUTTI GLI AUTORIZZATI

Gli autorizzati, nel trattare i dati personali e, dovranno operare garantendo la massima riservatezza ed integrità delle informazioni.

In particolare il dipendente, nell'ambito del suo rapporto di lavoro pubblico, nonché i Componenti gli Organi Istituzionali e le Commissioni dell'Ente, rispettano 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 mantengono 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. Osservano inoltre il dovere di riservatezza anche dopo la cessazione dal servizio e alla scadenza della carica. Non forniscono informazioni in merito ad attività istruttorie, ispettive o di indagine in corso presso l'Ufficio e non rilasciano informazioni relative ad atti e provvedimenti prima della loro comunicazione alle parti. Non fanno 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 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 documento. Le ulteriori disposizioni sono indicate nei singoli atti di nomina.

4 USO DEGLI STRUMENTI E RELATIVE ISTRUZIONI

Gli autorizzati sono tenuti ad operare e custodire i beni e gli strumenti (Banche dati, applicativi ecc.) a loro affidati adottando le cautele necessarie al mantenimento della loro efficienza ed integrità adottando tutte le misure di sicurezza messe a disposizione dall'Ente anche qualora effettuino la prestazione in modalità agile o da remoto.

Gli strumenti affidati sono nella disponibilità del soggetto autorizzato primariamente per un fine di carattere istituzionale e/o lavorativo.

4.1 REGOLE PER LA GESTIONE DELLE PASSWORD

Gli autorizzati devono accedere alla rete, ai sistemi di file sharing utilizzati e quindi alle varie attività di trattamento dei dati, utilizzando metodi di autenticazione per garantire l'accesso protetto secondo il livello di protezione scelto e deciso dall'Ente. Le credenziali di autenticazione

per l'accesso ai sistemi, assegnate agli autorizzati, possono consistere in: parole chiavi dette "password", codici per l'accesso, eventuali certificati digitali, i token per la generazione automatica di codici, ecc..

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 trimestrale o quando ritenga che, per qualunque motivo, abbia perso le caratteristiche di segretezza;
- La parola chiave 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:
  - lunghezza non inferiore a quanto richiesto dall'amministratore di sistema;
  - 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, 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 o cessazione dalla, carica 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.

4.2 DISPONIBILITÀ DI DATI O STRUMENTI ELETTRONICI IN CASO DI ASSENZA

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.

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 dal Direttore dell'Ente che ne avrà autorizzato l'esecuzione e che darà immediata notizia all'autorizzato al suo rientro.

4.3 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);
- impostare il sistema in modo che si blocchi automaticamente nel momento in cui l'operatore si allontana dalla postazione.

4.4 MISURE DI SICUREZZA

4.4.1 ANTIVIRUS E PROTEZIONE DA PROGRAMMI PERICOLOSI

L'uso di programmi antivirus è obbligatorio per tutti i dispositivi (PC, Notebook, tablet e smartphone) collegati, anche temporaneamente in rete.
Tutti i PC, Notebook o altri dispositivi, 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. Non sono consentiti l'apertura, il salvataggio, la registrazione, l'apertura o l'esecuzione di file "allegati" ricevuti in e-mail da mittenti sconosciuti o sospetti.

4.4.2 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"*).

4.4.3 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.

4.4.4 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.

4.4.5 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 in via prioritaria nel cloud e su supporti rimovibili (NAS). La frequenza delle copie è giornaliera, anche su dispositivi diversi e con modalità diverse.

4.4.6 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;

La password sarà assegnata dall'amministratore di sistema in accordo con il funzionario preposto dell'Ente e dovrà essere conservata secondo la procedura già in atto per le password.
Ove necessario periodicamente l'amministratore di sistema provvede alla sostituzione della password 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) verrà predisposto un utente per autenticazione comune la cui password sarà variata regolarmente almeno ogni sei mesi. In tali pc non devono essere conservati dati personali particolarmente riservati. Questi portatili con le autenticazioni assegnate a uso comune

non potranno accedere alla rete LAN dell'ordine ma avranno accesso solo alla navigazione Internet.

4.4.7 LICENZE D'USO DEI PROGRAMMI SOFTWARE

È 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", dovrà essere comunicata ed autorizzata dall'Ente sentito l'RTD e l'ADS.

4.4.8 INTERNET E POSTA ELETTRONICA

Per il personale in servizio la navigazione in Internet è inerente a scopi strettamente legati all'attività lavorativa, fatto l'utilizzo eccezionale e limitato nel tempo per necessità personali che non vadano e ledere l'efficacia dell'attività amministrativa dell'Ente.

È vietato:

-accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, che siano in qualche modo discriminatori;

- scaricare software (anche gratuito) da siti internet;

-effettuare transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo per attività lavorative;

-effettuare qualsiasi registrazione a siti internet i cui contenuti non siano riconducibili all'attività lavorativa;

-archiviare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di internet, nonché un possibile illecito trattamento di dati personali, è ricondotta nella responsabilità personale del soggetto inadempiente.

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 in eccesso. 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 attachment 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.

Il personale in servizio è responsabile del contenuto delle proprie comunicazioni ed è tenuto ad utilizzare un linguaggio rispettoso della propria posizione istituzionale degli organi politici e dei colleghi anche per quanto riguarda la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare la violazione dell'obbligo di fedeltà, del segreto d'ufficio e della normativa per la tutela dei dati personali.

4.4.9 CONVERSAZIONI TELEFONICHE

Non è consentito fornire informazioni riservate sugli iscritti dell'Ordine, fornitori 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.

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. Evitando le conversazioni a viva-voce.

4.4.10 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 solo alle persone appositamente autorizzate.

4.4.11 CIFRATURA

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

4.4.12 CUSTODIA E RIUTILIZZO DEI SUPPORTI RIMOVIBILI

È tendenzialmente sconsigliato l'uso di supporti rimovibili (es. chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati) per l'attività dell'Ente in quanto le difficoltà di gestire efficacemente l'importazione e l'esportazione di dati potrebbe esporre l'Ente a svariati rischi di perdite di dati o di introduzione nel sistema informatico di attacchi informatici.

Gli autorizzati, ai quali è stato permesso il trattamento del dato tramite l'utilizzo di supporti rimovibili (forniti esclusivamente dall'Ente e dei quali si prevede la registrazione del soggetto cui vengono affidati in segno di assunzione di responsabilità), 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).

4.4.13 USO STAMPANTI

L'Ente mette a disposizione di dipendenti e collaboratori unità periferiche di stampa ad uso esclusivamente istituzionale e lavorativo. I dipendenti e collaboratori sono tenuti ad effettuare la stampa dei dati solo se necessaria all'attività lavorativa e a ritirarla prontamente dai vassoi delle stampanti comuni, in modo da evitare che sia visibile o possa essere raccolta da terzi.

4.4.14 CLOUD COMPUTING

Con il termine cloud computing si indica uno strumento di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on-demand attraverso Internet a partire da un insieme di risorse/dati preesistenti e configurabili. Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Ente a potenziali rischi di violazione della privacy. I dati personali vengono memorizzati nelle server farm di aziende che spesso risiedono in uno stato extraeuropeo, configurando un trasferimento dei dati all'estero.

È perciò vietato l'utilizzo di sistemi Cloud non espressamente approvati dall'Ente se possibile, previo parere del DPO, nel rispettivo di specifiche procedure di controllo che verifichino i requisiti di affidabilità sicurezza informatica e di protezione dei dati personali.

5 ARCHIVI CARTACEI

Gli autorizzati sono tenuti a garantire sempre la corretta custodia dei documenti dell'Ente a loro affidati adottando le cautele necessarie al mantenimento della loro integrità adottando tutte le misure di sicurezza messe a disposizione dall'Ente assicurando:

- che i documenti non vengano lasciati incustoditi sulle scrivanie e/o in luoghi aperti al pubblico in assenza di altri autorizzati medesimo trattamento; i documenti non possono essere riprodotti o fotocopiati, se non per esigenze connesse alle finalità del trattamento; i documenti non devono essere consultati da persone non autorizzate al trattamento;
- di conservare i documenti o gli atti, che contengono dati particolari e/o giudiziari, in archivi ad accesso controllato, come ad es. armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di autorizzati;
- restituire tempestivamente la documentazione prelevata dagli archivi, al termine delle operazioni di trattamento;
- in caso di utilizzo di stampanti, fotocopiatrici o fax, condivisi da vari utenti e collocati al di fuori dei locali ove è posta la propria postazione di lavoro, raccogliere e custodire immediatamente, con le modalità sopra descritte, tutte le stampe prodotte;
- distruggere opportunamente le copie cartacee non più utili di documenti contenenti dati personali, evitando di gettarli via così come sono;
- adottare misure che siano idonee a limitare la conoscenza dei dati particolari e/o giudiziari qualora essi siano presenti nei flussi documentali dell'Amministrazione, garantendo il rispetto della riservatezza dei dati degli interessati.

6 DISPOSIZIONI FINALI

Le presenti Linee Guida costituiscono 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 ma tenendo in debito conto che l'Ente nell'ambito della sua attività tratta anche dati cartacei che possono essere memorizzati o transitare per apparecchiature digitali.

Tutto il personale dipendente, le persone in *stage* o somministrazione*,* i Componenti degli Organi Istituzionali e delle Commissioni dell'Ente, i consulenti, i collaboratori esterni, gli addetti alla manutenzione e alla gestione di strumenti elettronici, sono tenuti a rispettare le presenti Linee Guida scrupolosamente, nell'ambito delle proprie competenze ed attività e nei rapporti anche con soggetti terzi.

La violazione parziale o totale delle presenti Linee Guida potrà essere suscettibile di provvedimenti disciplinari commisurati alla gravità della violazione, oltre che alle sanzioni civili, penali nonché disciplinari previste dalla vigente normativa e declinate all'interno del Codice di Comportamento dell'Ente.

Anche 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 documento.