SERVIZIO SANITARIO REGIONALE
Dipartimento Tutela della Salute e Politiche Sanitarie

Azienda ospedaliero-universitaria
MATER DOMINI
CATANZARO

REGIONE CALABRIA

DISCIPLINARE SULLA PROTEZIONE DELLE PERSONE FISICHE RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI POLICY GENERALE

REGOLAMENTO (UE) 2016/679 – D.LGS. N. 196/2003)

L'**Azienda ospedaliero-universitaria Mater Domini**, con sede in con sede in Catanzaro (Italy), Via Tommaso Campanella n. 115 (di seguito: **Titolare del trattamento** o **Titolare**), ai sensi del D.Lgs. n. 196/2003 e del Regolamento Generale sulla protezione dei dati personali – Regolamento (UE) 2016/679 (RPD o GDPR) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, adotta il presente documento, denominato «Disciplinare sulla protezione delle persone fisiche riguardo al trattamento dei dati personali – Policy generale» (di seguito anche: **Disciplinare**).

Art. 1
Normativa di riferimento

Il presente disciplinare è redatto in conformità alla sottoscritta normativa:

1) Legge n. 241/1990 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi);
2) D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali);
3) D.Lgs. n. 82/2005 (Codice dell'Amministrazione Digitale – CAD);
4) D.Lgs. n. 33/2013 e D.Lgs. n. 97/2016 (Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni);
5) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (RGDP o GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
6) D.Lgs. n. 101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679);

Art. 2
Definizioni

RPD o GDPR	Regolamento sulla Protezione dei Dati o General Data Protection Regulation n. 679 del 2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
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
Dati particolari	i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Dati relativi alla salute	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
Dati genetici	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
Dati biometrici	dati personali ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale, l'impronta digitale o i dati dattiloscopici
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
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

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 per la protezione dei dati (DPO)	il soggetto designato dal Titolare del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative ed informative relativamente all'applicazione del GDPR. Coopera con l'Autorità (Garante per la protezione dei dati personali) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali
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. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento
Terzo	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile
Autorizzazione	le operazioni alle quali un soggetto è autorizzato al trattamento in base alle mansioni ricoperte e/o ai privilegi riconosciuti dal sistema informatico aziendale
Designato/autorizzato	la persona fisica cui il titolare o il responsabile del trattamento attribuiscono specifici compiti e funzioni connessi al trattamento dei dati personali
Limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro
Profilazione	qualsiasi forma di trattamento automatizzato 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
Pseudonimizzazione	il trattamento dei dati personali in modo tale che i dati personali 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
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

Art. 3
Ambito di applicazione e sanzioni

1. Il presente Disciplinare si applica a tutti i trattamenti dei dati personali posti in essere dall'**Azienda ospedaliero-universitaria Mater Domini**.
2. Il trattamento dei dati personali è consentito esclusivamente ai soggetti designati/autorizzati, ai Responsabili del trattamento ed eventuali Sub-Responsabili del trattamento, nonché agli Amministratori di Sistema.
3. Il trattamento effettuato da soggetti a ciò non preventivamente e formalmente autorizzati è illecito.
4. Con il presente documento l'**Azienda ospedaliero-universitaria Mater Domini** fornisce dettagliate procedure ed istruzioni per il trattamento dei dati personali da parte dei soggetti designati/autorizzati, ai sensi degli artt. 28 e 29 del GDPR e dell'art. 2quaterdecies del D.Lgs. n. 196/2003.
5. L'inosservanza delle disposizioni contenute nel presente Disciplinare e/o nei singoli atti di designazione/autorizzazione costituisce grave violazione, perseguibile ai sensi di legge e di contratto, e può comportare l'applicazione di sanzioni disciplinari, oltre che di natura penale.

Art. 4
Delegati autorizzati al trattamento

1. La funzione di delegato/autorizzato è attribuita dal Titolare del trattamento con atto formale, sottoscritto dal destinatario e contenente eventuali istruzioni dettagliate ulteriori rispetto a quelle indicate nel presente Disciplinare.
2. I delegati/autorizzati sono organizzati secondo livelli e profili differenziati, anche per materia, tenuto conto della struttura funzionale ed organizzativa del Titolare (organigramma).
3. Possono essere delegati/autorizzati i soggetti che, a qualsiasi titolo, prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Azienda in attività che comportano il trattamento di dati personali per conto del Titolare. (es. tirocinanti, studenti, stagisti, volontari, libero professionisti, borsisti, consulenti, ecc.).
4. Il Titolare conserva l'elenco dei soggetti designati/autorizzati e copia degli atti di designazione a delegato/autorizzato al trattamento dei dati personali.
5. Relativamente alla propria Area di competenza o Ufficio, il delegato/autorizzato che sia dotato di autonomia gestionale ed organizzativa risponde al Titolare di ogni violazione o mancata attivazione di quanto previsto nel presente Disciplinare e, in particolare, dell'inosservanza delle istruzioni impartite dal Titolare in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale.

6. Ciascun delegato/autorizzato:
   - adotta le istruzioni al trattamento e le indicazioni di comportamento ricevute dal Titolare, anche con riferimento al personale e agli utenti;
   - collabora con il Titolare, il Responsabile della protezione dei dati (DPO), i Responsabili del trattamento ed eventuali Sub-Responsabili, gli Amministratori di sistema, nonché con gli altri designati/autorizzati;
   - accede esclusivamente ai dati personali per i quali ha ricevuto apposita autorizzazione, osservando scrupolosamente il divieto di trattare dati personali estranei all'Area/Reparto/Ufficio di competenza;
   - verifica l'esattezza, l'aggiornamento, la pertinenza e la congruità dei dati personali trattati, in relazione all'attività svolta;
   - limitatamente ai propri ambiti di competenza, effettua l'analisi dei rischi afferenti al trattamento dei dati personali e alla conservazione dei medesimi, secondo le istruzioni impartite dal Titolare;
   - informa, senza ingiustificato ritardo, il Titolare o il Responsabile per la protezione dei dati personali (DPO) del verificarsi di una violazione dei dati personali, fornendo la massima collaborazione al fine di soddisfare le indicazioni di cui agli artt. 33 e 34 del GDPR.

Art. 5
Princìpi generali

1. Il trattamento dei dati personali dovrà avvenire rispettando e facendo rispettare i **principi di riservatezza**, **correttezza**, **liceità** e **trasparenza** richiesti dal GDPR e dal D.Lgs. n. 196/2003, nonché attenendosi alle istruzioni (policy, regolamenti, ecc.) impartite dal Titolare del trattamento.
   In particolare, all'interno delle sedi dell'Azienda la riservatezza dell'interessato è garantita attraverso specifiche misure, quali:
   - adozione di distanze di cortesia presso gli sportelli
   - divieto di chiamare ad alta voce i pazienti in attesa del proprio turno
   - riservatezza nei colloqui con pazienti e/o familiari
   - divieto di divulgazione, con qualsiasi forma e mezzo, dei dati personali dei pazienti
   - divieto di esporre nei reparti o in altri locali aperti al pubblico liste di pazienti in stato di ricovero ovvero in attesa di intervento
   - divieto di fornire notizie sensibili in situazioni di promiscuità o in presenza di personale estraneo o non autorizzato
   - utilizzo di paraventi o simili al fine di limitare la visibilità del malato ai soli familiari o conoscenti, all'interno dei reparti di terapia intensiva e, ove disponibili, di tutti i reparti.
2. Il trattamento dei dati personali dovrà altresì avvenire esclusivamente per le **finalità** indicate dal Titolare e per lo svolgimento delle mansioni affidate.
3. Il trattamento dei dati personali consentirà l'accesso unicamente ai dati ed alle **banche dati** necessarie per svolgere le attività di trattamento che rientrano nell'ambito delle mansioni assegnate al designato/autorizzato, utilizzando gli strumenti messi a disposizione dal Titolare secondo le autorizzazioni assegnate.
4. L'accesso ai dati personali durerà per il **tempo** strettamente necessario al perseguimento delle finalità del trattamento.
5. I dati personali sono trattati soltanto qualora siano **essenziali** e **necessari** allo svolgimento delle attività in capo al Titolare e nel caso in cui tali attività non possano essere adempiute mediante il trattamento di dati pseudonimizzati, fatto salvo in ogni caso il diritto all'anonimato nei casi previsti dalle normative vigenti.
6. Se necessario, i dati devono essere aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
7. I dati che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari, non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
8. La **comunicazione a terzi** dei dati personali trattati non è consentita, salvo che la comunicazione sia indispensabile per lo svolgimento dell'attività e avvenga nei confronti di terzi autorizzati dal Titolare del trattamento, oppure avvenga nei confronti di organi giurisdizionali o nell'adempimento di norme di legge, di regolamenti, di provvedimenti delle autorità, fatta salva in ogni caso diversa istruzione del Titolare.
9. I dati personali sono **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, salvo che vengano conservati per periodi più lunghi ai soli fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'osservanza delle misure tecniche e organizzative disposte dal Titolare a tutela dei diritti e delle libertà dell'interessato.
10. L'**aggiornamento** e/o la **distruzione** dei dati detenuti dovrà avvenire tenuto conto degli obblighi legali di conservazione secondo le istruzioni ricevute dal Titolare del trattamento. E' fatto assoluto divieto di asportare i supporti informatici o cartacei contenenti dati personali, senza la preventiva autorizzazione del Titolare.
11. Il designato/autorizzato ha l'obbligo di aderire ai **programmi di formazione** organizzati e curati dal Titolare del trattamento in materia di protezione e sicurezza dei dati personali. E' altresì tenuto al rispetto scrupoloso di tutte le misure di **sicurezza** adottate dal Titolare del trattamento.
12. Il designato/autorizzato si obbliga a mantenere la più assoluta **riservatezza** sui trattamenti effettuati, sia in costanza del rapporto – di qualsivoglia natura – con il Titolare, sia dopo la conclusione dello stesso. A tal fine, si impegna a non divulgare a terzi (compresi familiari, amici e conoscenti) le suddette informazioni, adottando ogni più opportuna precauzione al fine di impedirne eventuali comunicazioni e/o diffusioni.
13. Il designato/autorizzato si impegna ad impedire con **misure idonee** (es. password complesse) l`accesso alle persone non autorizzate agli strumenti (pc, tablet, ecc.) ricevuti in dotazione dal Titolare o di proprietà personale contenenti informazioni riservate di proprietà del Titolare del trattamento.
14. Il Titolare del trattamento fornisce le istruzioni a ciascun designato/autorizzato anche per il tramite di messaggi di posta elettronica o comunicazioni informali.
15. Il Titolare pone in essere, anche periodicamente, di concerto con il Responsabile per la protezione dei dati personali (DPO), attività di verifica e controllo del rispetto delle misure di legge e delle ulteriori disposizioni impartite durante le operazioni di trattamento dei dati personali da parte dei Responsabili del trattamento ed eventuali Sub-responsabili, Amministratori di Sistema e designati/autorizzati al trattamento.

Art. 6
Trattamenti mediante l'ausilio di strumenti elettronici

1. Le istruzioni contenute nel presente articolo sono applicabili a tutti i trattamenti posti in essere dal designato/autorizzato mediante l'utilizzo di strumenti informatici ed elettronici, inclusi quelli effettuati mediante gli applicativi gestionali forniti dal Titolare.

2. Il designato/autorizzato è in possesso di credenziali di autenticazione d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e di accesso ad Internet, che consistono in un codice di identificazione (user-id) associato ad una parola chiave riservata (password). Per specifici trattamenti, il Titolare può prevedere l'utilizzo di dispositivi di autenticazione (es. smart card), anche con caratteristiche biometriche.
3. Le credenziali di accesso alla rete ed ai sistemi, nonché qualsiasi altra informazione legata al processo di autenticazione, devono essere conservate nella massima segretezza e non possono essere divulgate. In caso di perdita, di inutilizzo delle credenziali per un periodo superiore a 3 (tre) mesi o di cessazione del rapporto – di qualsivoglia natura – con il Titolare, le credenziali di accesso saranno disattivate.
4. L'accesso ai PC avviene mediante password personale, scelta dal designato/autorizzato secondo criteri rispondenti alle normative aziendali e alle presenti istruzioni. Su autorizzazione del Titolare, può essere impostata una password di BIOS.
5. Nella scelta della **password**, il designato/autorizzato dovrà osservare le seguenti indicazioni:
   - usare almeno 8 caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito;
   - usare lettere, numeri e almeno un carattere speciale (es. # $! @ - > <);
   - non utilizzare riferimenti agevolmente riconducibili al designato/autorizzato (es. date di nascita, nomi o cognomi propri o di parenti);
   - non impostare come password la matricola o l'user-id;
   - custodire la password sempre in un luogo sicuro e non accessibile a terzi, senza divulgarla o condividerla con altri utenti o terzi;
   - non rivelare le password al telefono, né inviarla via fax, mail o altro mezzo;
   - non far digitare la password a soggetti estranei, incluso il personale di assistenza tecnica;
   - aggiornare periodicamente la password, con cadenza almeno mensile.
6. Costituiscono specifici **obblighi** del designato/autorizzato:
   A. trattare i dati personali utilizzando unicamente i software offerti e/o indicati dal Titolare (videoscrittura, fogli di calcolo, basi di dati, publishing, presentazioni, video editing, ecc.);
   B. non eseguire, se non previa esplicita autorizzazione del Titolare del trattamento, copie o back-up di sicurezza dei dati su spazi e supporti diversi da quelli indicati dal Titolare;
   C. utilizzare esclusivamente i programmi forniti dal Titolare come antivirus, antimalware, antispyaware, firewall e ogni altro applicativo idoneo a garantire la massima misura di sicurezza;
   D. verificare costantemente che i profili di accesso assegnati alle persone autorizzate al trattamento siano adeguati e non eccedenti le esigenze della mansione o dell'Unità organizzativa/operativa cui gli stessi sono stati assegnati;
   E. custodire le credenziali di accesso alle reti e ai sistemi informatici offerti dal Titolare in luogo sicuro e non accessibile a soggetti diversi dalla persona autorizzata all'accesso;
   F. utilizzare esclusivamente le caselle di posta elettronica messe a disposizione dal Titolare.
7. Il designato/autorizzato dovrà porre in essere ogni attività utile al continuo e completo aggiornamento dei **software antivirus** ed è tenuto a controllare la presenza ed il regolare funzionamento sul PC in dotazione del software antivirus aziendale. Nel caso in cui quest'ultimo rilevi un virus che non è riuscito a ripulire, il designato/autorizzato dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer, e segnalare immediatamente l'accaduto al Titolare.
8. I **PC portatili** assegnati al Designato per ragioni di servizio:
   - devono essere custoditi in un luogo protetto laddove siano utilizzati all'esterno (es. in occasione di convegni, trasferte o servizio esterno)
   - e, comunque, in caso di allontanamento;
   - non devono essere in alcun caso lasciati incustoditi
   - devono contenere sul disco esclusivamente i files strettamente necessari ai trattamenti eseguiti per ragioni di servizio
   - devono essere collegati periodicamente alla rete interna, a cura del Designato, per consentire il caricamento dell'aggiornamento dell'antivirus, antimalware, antispyaware, firewall e ogni altro applicativo idoneo a garantire la sicurezza.
9. Deve essere effettuato, con cadenza almeno settimanale, un salvataggio di back-up di eventuali dati personali presenti unicamente su PC portatili o comunque non accessibili tramite i sistemi informatici aziendali.
10. I dati personali conservati sui PC devono essere **cancellati** in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.
11. In linea generale, è vietata la **copia su supporti esterni** (CD, DVD, supporti USB) di dati personali, senza preventiva autorizzazione del Titolare. Ove nello svolgimento della normale attività lavorativa assegnata al designato/autorizzato – nell'ambito del suo profilo di autorizzazione – il Titolare abbia autorizzato la copia di dati personali, è opportuno ricorrere all'uso di supporti (CD, DVD, supporti USB) attenendosi alle seguenti cautele:
    A. accertarsi che il supporto sia debitamente formattato e privo di altri files, che potrebbero essere infetti;
    B. al fine di evitare l'alterazione dei dati in questione, dopo la copia sul supporto, dovrà essere attivata la protezione contro possibili nuove scritture, che potrebbero alterare i dati stessi;
    C. prima dell'utilizzo, il supporto deve essere verificato mediante software antivirus aziendale e, in caso di esito negativo, non potrà essere utilizzato;
    D. il supporto deve essere contrassegnato da un'etichetta, con una indicazione in chiaro o in codice, tale da permettere alle persone autorizzate al trattamento di quei dati di riconoscere immediatamente il contenuto del supporto;
    E. il supporto contenente dati personali deve essere sempre direttamente e personalmente custodito dal designato/autorizzato che ha realizzato la copia;
    F. in caso di spedizione ad altro designato/autorizzato, occorre accertarsi che il destinatario abbia lo stesso profilo di autorizzazione del mittente e che il supporto venga spedito in busta sigillata, intestata personalmente al designato/autorizzato ricevente, con controfirma sul lembo di chiusura;
    G. non si deve consentire l'accesso, trasmettere o spedire un supporto contenente dati personali ad un destinatario, senza avere prima concordato con lo stesso le modalità e i tempi di consegna ed avere stabilito la procedura, che deve permettere di confermare l'avvenuta consegna al destinatario;
    H. qualora i dati contenuti sul supporto non abbiano più ragione di essere, si deve provvedere immediatamente alla sua formattazione e contestuale asportazione o cancellazione dell'etichetta indicante il contenuto;
    I. il supporto non deve essere mai avvicinato ad un campo magnetico, né esposto ad estremi di temperature e di umidità;
    J. terminata la copia, il supporto non deve essere lasciato inserito nel PC, né deve mai essere lasciato abbandonato sul tavolo, ma va posto all'interno di una custodia sicura, preferibilmente all'interno di un cassetto della scrivania chiuso a chiave, in un armadio blindato ovvero in altro luogo non liberamente accessibile a persone estranee al Designato/autorizzato;
    K. qualora il contenuto del supporto debba essere copiato su un hard disk o altro strumento elettronico di trattamento, occorre accertarsi di cancellare il relativo contenuto al termine dell'operazione di trattamento, in modo che l'asportazione dei dati registrati

dal supporto sia completa;

L. si raccomanda di compilare un **registro** con l'indicazione numerica, o con altro contrassegno, ove sono riportati tutti i supporti contenenti dati sensibili, la loro ubicazione, le modalità di accesso e gli eventuali estremi di consegna ad altro designato/autorizzato.

12. E' fatto divieto di condividere cartelle in rete, dotate o meno di password, se non dietro esplicita e formale autorizzazione del Titolare.

Art. 7
Trattamenti senza l'ausilio di strumenti elettronici

1. La gestione dei dati personali ha luogo anche attraverso l'impiego di schede, fascicoli e altri documenti cartacei.
2. I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.
3. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.
4. I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassetti chiusi a chiave, se disponibili) e non devono comunque rimanere incustoditi su scrivanie o tavoli di lavoro.
5. I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
6. Non devono mai essere lasciati incustoditi fascicoli, incartamenti, corrispondenza, schede o altri documenti contenenti dati personali.
7. Il designato/autorizzato avrà cura di non cestinare documenti cartacei contenenti dati personali, o loro copie, senza averli prima distrutti in maniera opportuna, utilizzando – ove presente – apposita apparecchiatura distruggi documenti.
8. In caso di errore nell'esecuzione di una fotocopia di un documento che contiene dati personali, questa potrà essere cestinata solo dopo essere stata distrutta.
9. In caso di errore nella scansione su file di un documento contenente dati personali, questa dovrà essere eliminata definitivamente dal PC senza transitare nel cestino.
10. Il designato/autorizzato dovrà ritirare senza ritardo i documenti cartacei contenenti dati personali e stampati mediante l'utilizzo di stampanti condivise.

Art. 8
Utilizzo di internet e della posta elettronica

1. L'utilizzo di internet da parte del designato/autorizzato deve avvenire esclusivamente per finalità attinenti alla prestazione richiesta dal Titolare, con divieto di scaricare dalla rete files e software di uso non direttamente riferibile all'attività di lavoro, in quanto i software necessari all'attività lavorativa dovranno essere richiesti alle competenti strutture del Titolare.
2. Nell'utilizzo della posta elettronica, al fine di evitare situazioni di pericolo per i dati contenuti nel PC in dotazione, il designato/autorizzato:
   - non deve scaricare software gratuiti e shareware prelevati da siti internet, se non espressamente utili all'attività istituzionale dell'Ente e previa autorizzazione delle competenti strutture del Titolare.
   - non deve utilizzare software pear to pear (P2P) per il download di qualunque tipo di file (es. Emule).
   - non deve, neanche utilizzando pseudonimi, partecipare a forum non professionali, utilizzare chat line o bacheche elettroniche, registrarsi in guest books;
3. La posta elettronica è un mezzo di comunicazione messo a disposizione del designato/autorizzato esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, con riferimento sia alla "casella di posta elettronica dell'ufficio o istituzionale", sia alla "casella di posta elettronica individuale".
4. Nell'utilizzo della posta elettronica, al fine di evitare situazioni di pericolo per i dati contenuti nel PC in dotazione, il designato/autorizzato:
   - non deve accedere a caselle personali diverse da quella aziendale;
   - non deve installare client di posta elettronica in locale (es. Microsoft Outlook);
   - non deve aprire messaggi con allegati di origine dubbia, ignota o comunque non accreditata dal Titolare, nonché filmati e presentazioni non attinenti l'attività lavorativa;
   - deve cancellare, senza aprirli, i messaggi e/o i relativi allegati provenienti da mittenti sconosciuti o, anche se provenienti da mittente conosciuto, il cui contenuto è sospetto;
   - deve utilizzare un formato protetto da scrittura (es. PDF/A) nel caso in cui debba inviare un documento all'esterno dell'Ente;
   - può iscriversi a mailing list o newsletter esterne solo per motivi istituzionali, previa verifica sull'attendibilità del fornitore del servizio;
   - deve controllare i files allegati alla posta elettronica prima del loro utilizzo, senza eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.

Art. 9
Ambiente e postazione di lavoro

1. Il designato/autorizzato deve adottare la politica del "clean desk" (scrivania pulita), trattando dati cartacei solo se necessario e privilegiando, ove possibile, l'utilizzo degli strumenti informatici e digitali messi a disposizione dal Titolare.
2. In presenza di persone terze (ospiti, personale di servizio, soggetti non autorizzati al trattamento, ecc.), il designato/autorizzato dovrà farle attendere in luoghi in cui non siano presenti informazioni riservate o dati personali.
3. Il designato/autorizzato non dovrà lasciare la propria postazione non presidiata per periodi lunghi e avrà cura di tenere chiuso a chiave il proprio ufficio per tutta la durata dell'assenza, così da evitare indesiderati o indebiti accessi ai locali in cui si svolge l'incarico assegnato ovvero in cui sono custoditi e trattati dati personali.
4. Se risulta necessario allontanarsi dalla propria postazione, il designato/autorizzato dovrà riporre i documenti cartacei e attivare il salvaschermo del PC in dotazione uscendo dalla sessione di lavoro.
5. Il designato/autorizzato deve impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia, da parte di persone non autorizzate, dei dati contenuti nei documenti cartacei che gli sono stati affidati in custodia.

Art. 10
Ulteriori adempimenti

1. Il designato/autorizzato verifica che agli interessati siano state fornite le informative predisposte dal Titolare del trattamento ai sensi degli artt. 12 e segg. del GDPR, avendo cura di raccogliere e archiviare il consenso in tutti i casi previsti dalla legge.

2. Il designato/autorizzato cura l'aggiornamento del Registro dei trattamenti, secondo le istruzioni ricevute dal Titolare del trattamento, offrendo a quest'ultimo ogni supporto utile e/o necessario per il corretto adempimento delle previsioni normative in materia di trattamento dei dati personali. In particolare informa prontamente il Titolare del trattamento:
   - di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
   - dell'eventuale necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute.
3. Il designato/autorizzato coordina e collabora con gli altri designati/autorizzati, attenendosi alle indicazioni fornite dal Titolare del trattamento e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri designati/autorizzati nei trattamenti effettuati.

Art. 11
Disposizioni finali

1. L'obbligo di ottemperare ai contenuti del presente Disciplinare è assunto dal designato/autorizzato a titolo non oneroso.
2. I contenuti del presente documento sono richiamati nei singoli Accordi di protezione dati sottoscritti, a norma dell'art. 28 del GDPR, con ciascun Responsabile del trattamento.
3. Il presente Disciplinare sostituisce eventuali documenti precedenti in materia di trattamento di dati personali con esso incompatibili, e produce effetti fino a successiva modifica e/o revoca del presente documento e, comunque, per tutta la durata delle funzioni e dei compiti assegnati ai singoli designati/autorizzati.
4. Il Titolare si riserva di adeguare, modificare o integrare il testo del presente Disciplinare per motivi organizzativi e/o in caso di eventuali modifiche normative.

Art. 12
Rinvio

1. Per tutto quanto non espressamente previsto dal presente Disciplinare, si applica la normativa vigente in materia di protezione dei dati personali e amministrazione digitale, come indicata all'art. 1 del presente documento.
2. Il Titolare si riserva di modificare, rettificare e/o integrare il presente Disciplinare alla luce delle eventuali innovazioni normative e delle azioni ritenute opportune e/o necessarie ai fini della responsabilizzazione in materia di protezione e tutela dei dati personali.