REGIONE TOSCANA
Società della Salute di Firenze
C.F. 94117300486
Piazza Signoria 1 – 50122 FIRENZE

PROVVEDIMENTO DEL DIRETTORE

Numero del provvedimento	75
Data del provvedimento	4 novembre 2025
Oggetto	Società della Salute
Contenuto	**APPROVAZIONE DISCIPLINARE INFORMATICO – ISTRUZIONI OPERATIVE PER IL TRATTAMENTO DEI DATI PERSONALI SU SUPPORTO INFORMATICO**

Ufficio/Struttura	Direzione Società della Salute
Resp. Ufficio/Struttura	Giuditta Giunti
Resp. del procedimento	Giuditta Giunti

Conti Economici			
Spesa	**Descrizione Conto**	**Codice Conto**	**Anno Bilancio**
Spesa prevista	**Conto Economico**	**Codice Conto**	**Anno Bilancio**

Allegati Atto		
Allegato	**N° di pag.**	**Oggetto**
1	12	Disciplinare informatico

Documento firmato digitalmente

REGIONE TOSCANA
Società della Salute di Firenze
C.F. 94117300486
Piazza Signoria 1 – 50122 FIRENZE

IL DIRETTORE

VISTO:

- che la legge regionale 24 febbraio 2005, n. 40, e ss.mm.ii. (“Disciplina del servizio sanitarioregionale”) e, segnatamente il capo III bis (“Società della Salute”), articoli 71 bis e ss. disciplina il nuovo assetto organizzativo dei servizi sanitari territoriali, sociosanitari e socialiintegrata tramite la costituzione delle Società della Salute;
- che in data 8 marzo 2010 è stata stipulata dagli enti consorziati la Convenzione della Società della Salute di Firenze, con allegato lo Statuto del Consorzio, entrato in vigore a seguito di detta stipula, già approvata dal Consiglio Comunale di Firenze e dal Direttore Generale dell’Azienda Sanitaria di Firenze;
- l’art. 12 dello Statuto che stabilisce le attribuzioni del Direttore della Società della Salute diFirenze;
- che con decreto del Presidente della Società della Salute di Firenze 15 ottobre 2025, n. 3, la sottoscritta, dott.ssa Giuditta Giunti, è stato nominata Direttrice del Consorzio e che l’incarico è decorso dal 20 ottobre 2025;

RICHIAMATO:

- il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR);
- il D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 101/2018;
- la necessità di adottare istruzioni operative per il trattamento dei dati personali effettuato mediante strumenti elettronici, in conformità all’art. 32 del GDPR;

CONSIDERATO CHE:

- è necessario disciplinare le modalità di trattamento dei dati personali su supporto informatico, al fine di garantire la sicurezza, la riservatezza, l’integrità e la disponibilità dei dati trattati;
- è stato predisposto il documento denominato “Disciplinare informatico – Istruzioni operative per il trattamento dei dati personali su supporto informatico”, allegatoal presente provvedimento quale parte integrante e sostanziale;

RITENUTO di dover procedere all’approvazione del suddetto disciplinare, quale misura organizzativa e tecnica a tutela dei dati personali trattati dalla Società della Salute di Firenze;

RITENUTO altresì opportuno, per motivi di urgenza, dichiarare la presente determinazione immediatamente eseguibile, ai sensi dell’art.42, comma quarto, della L.R.T. n. 40 del 24/02/2005 ess.mm.ii, vista la necessità di dare esecuzione al servizio;

DATO ATTO che l’istruttoria della presente delibera è stata curata dalla Dr.ssa Annagilda Gigliofiorito, Dirigente amministrativa della SdS, la quale attesta che la formazione del presente decreto è avvenuta nel rispetto degli obblighi di regolarità e correttezza dell’azione amministrativa;

PRESO ATTO del parere favorevole relativo alla regolarità tecnica del presente provvedimento, ai sensi dell'articolo 49, comma 1, del decreto legislativo n. 267/00;

Documento firmato digitalmente

REGIONE TOSCANA
Società della Salute di Firenze
C.F. 94117300486
Piazza Signoria 1 – 50122 FIRENZE

RICHIAMATO l'articolo 12 dello Statuto;

DISPONE

1. **Di approvare** il documento denominato *"Disciplinare informatico – Istruzioni operative per il trattamento dei dati personali su supporto informatico"*, allegato al presente provvedimento.
2. **Di disporre** che il disciplinare sia reso noto a tutto il personale dipendente e ai soggetti che, a vario titolo, trattano dati personali per conto della Società della Salute di Firenze.
3. **Di demandare** al Responsabile della Protezione dei Dati (DPO) il monitoraggio delle misure previste nel disciplinare.
4. **Di pubblicare** il presente provvedimento nella sezione "Amministrazione Trasparente" del sito istituzionale.
5. **Di trasmettere** il presente atto agli Enti aderenti ed al Collegio Sindacale.
6. **Di dare pubblicità** alla presente deliberazione mediante affissione all'Albo Pretorio del Consorzio, ove rimarrà per dieci giorni consecutivi, e mediante pubblicazione sul sito informatico della Società della Salute, ove resterà accessibile a tempo indeterminato.

Estensore: AnnagildaGigliofiorito

Il Provvedimento è firmato digitalmente da:

La Direttrice
Giuditta Giunti

Documento firmato digitalmente

	Documentazione di Sistema **Data Protection GDPR (Reg. UE 2016/679)** **Società della Salute Di Firenze**	Rif.	IST_01	Rev.	01
		Rev.		2025	
Istruzioni operative per il trattamento dei dati personali su supporto informatico (Disciplinare informatico)					

Indice

1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche, con il libero accesso ad *internet* ed alla posta elettronica da parte dei soggetti coinvolti nel trattamento, espone le organizzazioni (Società, Associazioni, ecc.) a rischi riguardanti la sicurezza dei dati nonché a potenziali rischi che possono offuscare l'immagine dell'organizzazione stessa.

Le precauzioni di tipo tecnico/informatico messe in atto dalla Società della Salute di Firenze (di seguito "SDS"), possono proteggere le informazioni sia durante la comunicazione attraverso i sistemi sia nella conservazione dei dati registrati su un disco fisso, ma nel momento in cui il trattamento informatico è effettuato da un utente incaricato, la loro protezione dipende sensibilmente dall'operato di quest'ultimo e nessuno strumento tecnologico può sostituirsi totalmente al suo senso di responsabilità, di etica e al rispetto di alcune semplici norme di comportamento.

Alcuni comportamenti degli Incaricati del trattamento che utilizzano le dotazioni informatiche possono minare la produttività del lavoro e favorire l'introduzione di codici malevoli (*virus, trojan, spyware*, ecc.) nella rete aziendale.

Il *Personal Computer* messo a disposizione dell'Incaricato è uno strumento di lavoro. Ogni utilizzo non inerente all'attività professionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza delle informazioni aziendali e, in particolare, dei dati personali degli Interessati.

Le presenti regole e istruzioni sono state redatte con la collaborazione del Responsabile della protezione dei dati designato dal Titolare, in conformità con il Regolamento UE 2016/679 (*General Data Protection Regulation* 2016/679 di seguito come GDPR).

Il presente documento potrà essere aggiornato compatibilmente con l'evoluzione della tecnologia informatica e le *policy* di sicurezza adottate dalla SDS.

2. Scopo e campo di applicazione

I principi riportati nel presente documento disciplinano specifiche regole di comportamento in relazione al trattamento di dati personali effettuato con modalità informatiche da parte degli Incaricati/autorizzati del trattamento a prescindere dalla natura contrattuale del rapporto di lavoro/collaborazione.

È opportuno richiamare alcune fondamentali definizioni contenute nella normativa citata:

- **Dato personale** (art. 4 n. 1 GDPR): "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".
- **Trattamento** (art. 4 n. 2 GDPR): "*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*".

3. Figure coinvolte nella protezione dei dati personali

La SDS ha progettato un sistema di gestione del trattamento dei dati personali conforme al *General Data Protection Regulation* - Reg.UE 2016/679.

In tale contesto il Titolare del trattamento si preoccupa di salvaguardare la riservatezza, la disponibilità e l'integrità delle informazioni aziendali e dei dati personali mettendo in atto misure tecniche, organizzative, informatiche e di natura legale e contrattuale atte a garantire la conformità delle sue attività ai requisiti cogenti contemplati dalla legge europea e dalle disposizioni italiane sulla protezione dei dati personali.

Al fine di favorire un lavoro costante, armonico, integrato nei processi aziendali e soprattutto per attivare efficaci meccanismi di comunicazione interna ed esterna e di sensibilizzazione del personale sull'importante e strategica tematica della protezione delle informazioni e dei dati personali, la SDS ha provveduto alla formale designazione di un Responsabile della Protezione dei Dati (RPD) che provvederà, d'intesa con la stessa, ad aggiornare periodicamente, ove necessario, le presenti indicazioni.

4. Utilizzo del *personal computer*

Per quanto attiene all'utilizzo delle apparecchiature informatiche, si evidenzia che l'Incaricato deve prestare la massima cura nella gestione delle stesse e attenersi rigorosamente alle seguenti disposizioni:

a) Utilizzare il *personal computer*, le stampanti e tutte le dotazioni di lavoro in modo da salvaguardarne l'integrità e il corretto funzionamento;

b) le risorse aziendali (*fax*, fotocopiatrice, *computer*, accesso ad *internet*, stampanti, ecc.) sono concesse in mero uso all'Incaricato per attività professionali e non per fini personali;

c) non è consentito installare autonomamente programmi esterni senza l'esplicita autorizzazione del Titolare del trattamento in quanto sussiste il grave pericolo di importare *Virus* informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dalla SDS. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il *software* esistente, può esporre la SDS a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul *software* che impone la presenza nel sistema di *software* regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. In merito si precisa che anche il *software freeware* spesso è tale solo per uso personale e non aziendale e pertanto soggetto a licenza d'acquisto;

d) è cura degli utilizzatori provvedere alla corretta archiviazione dei dati evitando di conservare i file sul *desktop* del *computer* ma utilizzando le cartelle di destinazione indicate dal Titolare;

e) non è consentito all'utente di modificare le caratteristiche di sistema (nome *computer*, indirizzi IP, DNS, *Firewall*, aggiornamenti automatici SW, etc.);

f) non è consentito connettere alla rete aziendale *Personal Computer* aziendali o di terzi in maniera autonoma non autorizzata dalla SDS. L'inosservanza di tale norma può essere causa di gravi rischi alla sicurezza e alla funzionalità aziendale in quanto se il *computer* portatile è infetto da *virus* o non dispone di idonei strumenti di protezione informatica può diventare l'anello debole della rete aziendale ed essere quindi fonte di minacce informatiche;
g) non è consentita l'installazione sul PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, *modem*, ecc.), se non con l'autorizzazione espressa della SDS;
h) non è consentito personalizzare i *desktop* dei propri *computer* con immagini personali;
i) non è consentito utilizzare chiavette USB o dischi esterni per la copia dei dati se non espressamente autorizzati dalla SDS;
j) non è consentito utilizzare servizi in *streaming* video o audio;
k) non è consentito masterizzare cd, dvd o dvx per finalità personali;
l) non è consentito lasciare incustodito e accessibile il *computer* durante una sessione di trattamento. In tal caso, disconnettere l'utente o terminare la sessione di lavoro con un *log out* ogni volta che ci si deve allontanare (anche per brevi periodi), evitando di lasciare la propria sessione di lavoro "aperta" ed accessibile a terzi non autorizzati;
m) non è consentito effettuare con il *computer* di lavoro trattamenti sui propri dati personali non attinenti alla sfera lavorativa (foto, comunicazioni personali, rubriche telefoniche, ecc.). In particolare, è assolutamente vietato trattare con il *computer* fornito in dotazione dalla SDS dati personali di natura sensibile attinenti alla sfera politica, religiosa, sessuale o inerente allo stato di salute dell'Incaricato;
n) attenersi scrupolosamente alle attività di copia, elaborazione, trasferimento dei dati previste dalle procedure aziendali in merito all'utilizzo dei programmi applicativi di pertinenza;
o) informare tempestivamente la SDS su potenziali rischi o problemi inerenti alla sicurezza informatica della postazione di lavoro assegnata.

5. Utilizzo delle stampanti, *fax* e fotocopiatrici

a) Assicurarsi di stampare le informazioni di natura sensibile o particolarmente riservata esclusivamente su stampanti presenti all'interno dei propri uffici o in uffici in cui gli Incaricati siano autorizzati al trattamento dei medesimi dati assicurandosi di non lasciare incustoditi i documenti sulla stampante;

b) Le stampanti, le fotocopiatrici e i *fax/telefax* sono beni della SDS e devono essere utilizzati dal personale esclusivamente per attività di carattere lavorativo e non per scopi di natura personale;

c) Assicurarsi di non lasciare documenti all'interno di fax, fotocopiatrici o stampanti;

d) Qualora si effettuino copie di documenti che contengono dati sensibili ma non sia necessaria la conoscenza di questi, l'Incaricato deve renderli illeggibili (con un pennarello nero) prima di porre il documento nella fotocopiatrice nel rispetto dell'art. 5 del GDPR 2016/679;

e) Presidiare la stampante, la fotocopiatrice o il *fax* quando il trattamento coinvolga dati sensibili o comunque strettamente riservati per evitare l'acquisizione indebita degli stessi da parte di soggetti non autorizzati.

Si evidenzia, tuttavia, che non è più ammesso, salvi casi di comprovata urgenza, l'uso del fax.

6. Utilizzo di supporti esterni

a) Tutti i supporti magnetici riutilizzabili (CD, DVD, supporti di memorizzazione USB) contenenti dati della SDS (ivi compresi quelli degli Interessati) devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere acquisito indebitamente da personale non autorizzato. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione;

b) I supporti magnetici contenenti dati sensibili (categorie particolari ex art. 9 Reg. UE 2016/679) e giudiziari (dati relativi a reati ex art. 10 Reg. UE 2016/679) devono essere custoditi in archivi chiusi a chiave;

c) Porre la massima attenzione alle chiavette USB per evitare possibili smarrimenti ed acquisizioni indebite di dati della SDS. Evitare di lasciare dati personali memorizzati nelle chiavette USB;
d) É vietato cestinare unità *storage* di dati esterne anche se obsolete o non funzionanti (dischi USB, dvd, cd, ecc.) che contenevano dati della SDS. Se non si attivano procedure atte a distruggere definitivamente i dati personali in essi contenuti, non viene esclusa la possibilità (anche se si tratta di supporti non funzionanti) che terzi acquisiscano indebitamente le informazioni in essi contenuti per finalità illegali. Nel caso di *hard disk* esterni o di *computer* obsoleti da smaltire, informare prontamente il Titolare;
e) É assolutamente vietato utilizzare chiavette USB trovate casualmente. I criminali informatici sfruttano le chiavette USB come "esche" per accedere indebitamente ai sistemi informativi delle aziende attraverso potenti "*rootkit*" non sempre rilevabili dagli *antivirus*;
f) Garantire sui supporti removibili tutte le misure atte ad evitare furti e acquisizione indebite da parte di terzi non autorizzati;
h) Informare tempestivamente la SDS su potenziali rischi o problemi inerenti alla sicurezza informatica dei supporti removibili utilizzati.

7. Utilizzo di *computer* portatili

a) Salvo specifica autorizzazione della SDS, non è concesso l'utilizzo di *computer* portatili personali (*laptop*, *netbook*, *tablet*) per finalità connesse al rapporto di lavoro/collaborazione con lo Stessa;
b) Ai *computer* portatili eventualmente autorizzati si applicano le stesse regole di utilizzo previste per i *computer* fissi connessi in rete;
c) É fatto espresso divieto all'Incaricato di archiviare dati personali degli Interessati della SDS sul proprio dispositivo portatile, anche se autorizzato.

8. Utilizzo della posta elettronica

a) La casella di posta, eventualmente assegnata dal Titolare all'Incaricato è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse;

b) É fatto divieto utilizzare la casella di posta elettronica aziendale per finalità personali;
c) É vietato accedere alla propria posta elettronica personale. Le *e-mail* e gli allegati alle stesse sono una potenziale e frequente fonte di *virus* che possono compromettere la sicurezza della rete informatica aziendale;
d) Non inviare o memorizzare *file* di natura oltraggiosa o discriminatoria;
e) É vietato trasmettere all'esterno documenti riservati della SDS;
f) La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti;
g) É obbligatorio controllare i *file* allegati di posta elettronica prima del loro utilizzo (non eseguire *download* di *file* eseguibili o documenti da siti *Web* o Ftp non conosciuti);
h) Salvo espressa autorizzazione da parte della SDS, non è consentito il "*redirect*" della propria casella di posta aziendale su *e-mail* personali;
i) É vietata ogni forma di comunicazione elettronica oltraggiosa, discriminatoria, offensiva, denigratoria nei confronti dei propri colleghi o personale della SDS;
l) Evitare di rispondere ad *e-mail* di provenienza dubbia;
m) Aprire solo gli allegati *e-mail* o dei messaggi istantanei provenienti da fonti attendibili e conosciute;
n) Non selezionare collegamenti *Web* inviati da sconosciuti;
o) É assolutamente vietato aprire allegati di *e-mail* di provenienza dubbia che fanno riferimento ad acquisti di *e-commerce*, corrieri per il ritiro di materiale o fantomatici rimborsi. La minaccia più grave e sempre più frequente è costituita dal *Cryptoloker*: un *ransomware* che blocca il funzionamento del *computer* criptando tutti i dati contenuti nell'*hard disk* (o nella partizione) infettato. I *virus* detti "*ransomware*" chiedono un riscatto per poter essere rimossi, si diffondono per *e-mail* e basta aprire un allegato per contrarre l'infezione;
p) É assolutamente vietato comunicare dati personali degli Interessati della SDS rispondendo a "fantomatiche" *e-mail* dell'autorità giudiziaria. La comunicazione dei dati degli Interessati all'autorità giudiziaria è fattibile solo dopo essersi accertati che la richiesta è effettivamente legittima ed ufficiale.

Ci sono criminali informatici, infatti, che utilizzano tecniche di *spoofing* inviando *e-mail* che falsificano l'identità del mittente per far credere al destinatario della comunicazione che l'*e-mail* è stata inviata da una fonte ufficiale attendibile.
In caso di assenza improvvisa o prolungata della persona assegnataria dell'indirizzo di posta, e comunque per improrogabili esigenze professionali, la SDS può accedere alla casella di posta del collaboratore per garantire la regolare esecuzione dei servizi e delle attività dell'organizzazione.
Si ribadisce pertanto che l'indirizzo di posta elettronica fornita dalla SDS deve essere utilizzato esclusivamente per finalità lavorative.

9. Utilizzo di *internet* e *social network*

La SDS non consente che venga utilizzato *internet* per fini strettamente personali, né tanto meno consente che venga effettuato l'accesso a siti *internet* a rischio in quanto potenziale fonte di *spyware*, *virus* ed attacchi informatici che possono minare l'integrità dei dati della SDS (ad esempio siti con contenuti erotici o pornografici, siti che permettono di scaricare giochi ed applicazioni gratuitamente, siti per suonerie di cellulari, ecc.).
Precisato quanto sopra, non è permesso:
a) navigare in siti non attinenti alle attività professionali;
b) navigare in siti che possono rivelare opinioni politiche, religiose, sindacali o sessuali;
c) partecipare per motivi non professionali a forum *on-line*, bacheche elettroniche e *guest book* anche utilizzando pseudonimi o *nickname*;
d) utilizzare *chat line*;
e) aggiornare il proprio profilo ed accedere a *social network* (*facebook*, ecc.) se non per finalità strettamente professionali;
f) registrarsi in siti non attinenti alle attività professionali (*newsletter*, *guest book*);
g) scaricare *software* gratuiti senza l'autorizzazione della SDS;
h) scaricare documenti informatici di natura oltraggiosa o discriminatoria o comunque che possono contenere opinioni politiche, religiose, sindacali o sessuali;

i) scaricare *file* musicali o video non attinenti alle attività professionali;
j) utilizzare servizi in *streaming* audio o video (*internet* radio, filmati, *youtube*, ecc.) che compromettono la banda disponibile causando perdite di efficienza della rete aziendale;
k) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote *banking*, acquisti *on-line* e simili salvo i casi direttamente autorizzati dalla SDS e con il rispetto delle normali procedure di acquisto;
l) quando si visita un sito *Web*, digitare l'indirizzo direttamente nel *browser* invece di fare clic su un collegamento;
m) fornire informazioni personali solo sui siti *Web* con connessione sicura "*https*" nell'indirizzo o con un'icona a forma di lucchetto nella parte inferiore del *browser*;
n) l'accesso a siti che contengono materiale pornografico;
o) utilizzare il nome della SDS per rappresentare opinioni personali attraverso *forum* di discussione di valenza pubblica;
p) scaricare materiale protetto dal diritto d'autore;
q) scambiare, pubblicare, caricare informazioni e/o dati personali e/o comunque riferiti alla SDS ivi comprese le immagini.

10. Utilizzo del telefono aziendale e del cellulare personale

I telefoni "fissi" e i cellulari aziendali, che la SDS eventualmente mette a disposizione per i suoi collaboratori, devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività professionale, secondo un utilizzo appropriato, efficiente, corretto e razionale.
Solo in caso di particolare necessità e/o urgenza, i collaboratori possono utilizzare tali beni per motivi personali non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.
La SDS si riserva di effettuare controlli in merito attraverso l'analisi dei tabulati del fornitore del servizio.
Per quanto riguarda il cellulare personale, fermo restando il buon senso e la buona educazione, si raccomanda di:
- evitare di utilizzare il cellulare personale nelle ore di ufficio se non per particolari necessità;

- evitare suonerie ad alto volume o con suoni “bizzarri”.

È tassativamente vietato l’utilizzo di servizi mobile o fissi (es. *whatsapp*) per scambiare informazioni, dati e/o documenti contenenti dati della SDS o degli Interessati della stessa.

11. Accesso alle dotazioni informatiche

Non è assolutamente consentito:

a) permettere ad un Interessato o a terzi non autorizzati di entrare negli uffici o negli ambienti della SDS ed utilizzare le dotazioni informatiche della stessa;

b) permettere di scaricare posta elettronica da parte di terzi non autorizzati;

c) collegare chiavette USB od altre interfacce esterne da parte di terzi non autorizzati;

d) permettere a terzi non autorizzati di accedere ad *internet* dalle postazioni di lavoro della SDS;

e) prestare all’Interessato *computer* portatili della SDS salvo espressa autorizzazione del medesimo.

12. Riservatezza dei *file*

a) Evitare di archiviare i *file* sul *desktop* e comunque in modo disordinato;

b) Nominare i *file* ed archiviarli opportunamente in *directory* che ne permettano un’immediata rintracciabilità;

c) Ricordarsi di aggiungere al nome del *file* l’indice di revisione (nomefile_rev1, nomefile_rev2, ecc.) se è necessario conservare la storicità degli aggiornamenti;

d) Evitare di nominare i *file* con nomi che riconducano direttamente ad informazioni di natura sensibile (es: lista_allergiealimentari.doc);

e) Impegnarsi nell’applicare (senza pregiudicare la corretta rintracciabilità delle informazioni) il principio di seguito indicato:

“I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od

opportune modalità che permettano di identificare l'interessato solo in caso di necessità";

f) Definire dei tempi di conservazione sui documenti elettronici;

g) Garantire il massimo livello di sicurezza e di riservatezza sui *file* contenenti dati di natura sensibile.

13. *Cloud computing* (nuvole virtuali)

L'utilizzo eventuale di tecnologie informatiche legate al *cloud computing* (in particolare quando si tratta di dati personali degli Interessati) dovrà essere condiviso e autorizzato dalla SDS.

In particolare, si dovranno avere idonee risposte in merito a:

1. chiara identificazione del fornitore *Cloud*;
2. affidabilità del fornitore del *Cloud*;
3. trasparenti clausole contrattuali;
4. identificazione della posizione fisica dei dati (il trasferimento di dati in Paesi che non offrono adeguate garanzie di sicurezza potrebbe comportare un illecito trattamento dei dati personali);
5. garanzie sulle misure di sicurezza e riservatezza sui dati;
6. garanzie sulla disponibilità dei dati in caso di necessità.

É assolutamente vietato trasferire dati personali fuori dall'Unione Europea se non nel rispetto delle specifiche istruzioni fornite dalla SDS.

14. Incidenti sulla sicurezza delle informazioni e dei dati personali

Qualsiasi incidente sulla sicurezza delle informazioni che implichi:

- la perdita di dati personali (esempio perdita di supporti fisici contenenti dati personali);
- la corruzione di dati personali (ad esempio *virus* o alterazione di dati personali);
- l'indisponibilità di accedere a dati personali e, più in generale, qualsiasi problema legato alla sicurezza delle informazioni e dei dati personali

deve essere prontamente comunicato alla SDS e al Referente *privacy*.

La SDS ha predisposto una procedura per la gestione degli incidenti sulla sicurezza delle informazioni (comprendendo dati personali) per rispondere in modo efficace con misure correttive idonee ad eventuali problemi che compromettano la riservatezza, disponibilità e integrità dei dati personali.
La misura in oggetto si è peraltro resa necessaria per rispondere ad un nuovo e puntuale obbligo contemplato dal GDPR 2016/679 che impone ai Titolari del trattamento di comunicare la violazione (cd. *data breach*), in determinate circostanze, all'Autorità Garante entro e non oltre le 72 ore dalla rilevazione di un incidente che può comportare pregiudizi per gli interessati.

15. Osservanza delle disposizioni in materia di *privacy*

È obbligatorio attenersi alle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali previste dal Regolamento UE 2016/679, dal D. Lgs. 196/2003 nonché dai provvedimenti del Garante per la protezione dei dati personali.
Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con le azioni civili e penali previste dalla legislazione vigente.

16. Lavoro agile o da remoto

Il presente documento intende disciplinare, altresì, l'utilizzo degli strumenti in dotazione al lavoratore e/o collaboratore nell'ipotesi in cui la prestazione lavorativa e/o di collaborazione all'interno della SDS venga eseguita in modalità lavoro agile o *smart-working*.
Il lavoro agile consiste nell'esecuzione della prestazione lavorativa e/o di collaborazione al di fuori della sede di lavoro assegnata, utilizzando, a tal fine, strumentazione informatica e/o telefonica idonea a consentire il corretto e tempestivo svolgimento della prestazione, nonché la comunicazione costante con la SDS, il Responsabile IT, i colleghi e tutti gli utenti interni ed esterni (a titolo esemplificativo gli utenti della SDS o i soggetti con i quali il Titolare tiene rapporti commerciali), sempre nel rispetto della normativa in materia di sicurezza dei dati e *privacy*.

La SDS garantisce al lavoratore e/o collaboratore che lavora da remoto la possibilità di eseguire la propria prestazione avvalendosi di strumenti informatici e/o telefonici (quali *personal computer*, *smartphone* e tutto quanto ritenuto opportuno) forniti dalla SDS stessa.
Il lavoratore e/o collaboratore, quindi, deve garantire il corretto utilizzo delle menzionate dotazioni strumentali che devono essere utilizzate al solo fine della prestazione lavorativa a favore della SDS e sempre nel rispetto delle presenti istruzioni di utilizzo, le quali si intendono integralmente richiamate anche in materia di lavoro agile.
Pertanto, il lavoratore e/o collaboratore garantisce che la strumentazione sarà utilizzata solo dallo stesso e che nessun soggetto non autorizzato potrà farvi accesso.
A tal fine, il lavoratore e/o collaboratore si impegna a custodire in modo diligente la strumentazione fornitagli, evitando qualsiasi situazione dalla quale potrebbe scaturire un pericolo per la funzionalità della dotazione o un accesso illegittimo alla stessa.
Nel caso in cui il lavoratore e/o collaboratore rilevi dei malfunzionamenti o delle attività sospette sugli strumenti informatici in dotazione, dovrà darne tempestivo avviso al Responsabile IT, così da minimizzare eventuali rischi per i dati ivi contenuti.

17. Controlli

Le finalità perseguite dalla SDS quale Titolare del trattamento richiedono che questa svolga e attivi comportamenti difensivi sul suo patrimonio informatico.
Rientrano tra le finalità del trattamento i dati che possono essere acquisiti (coinvolgendo anche consulenti od aziende esterne ufficialmente nominate) nell’ambito delle indagini difensive che la SDS adotta nella propria infrastruttura informatica e che possono far risalire a condotte illecite dell’Incaricato in violazione di questo disciplinare informatico interno e i dati personali acquisiti senza il consenso dell'Interessato alla luce di quanto previsto dall'art. 24, comma 1, lett. f), del Regolamento UE 2016/679 perché necessari ai fini dello svolgimento delle investigazioni difensive o, comunque, per far valere o difendere un legittimo diritto ed interesse del Titolare in sede

giudiziaria nel rispetto dei principi di pertinenza e non eccedenza rispetto alla finalità del trattamento.
Le attività di controllo del sistema informatico della SDS possono essere svolte dall'Amministratore di Sistema e dal *Data Protection Officer*.

18. Aggiornamenti

Il Titolare del trattamento potrà apportare revisioni e/o aggiornamenti al presente documento che verranno prontamente comunicati agli Incaricati e che, per effetto del vincolo contrattuale, si impegnano a rispettarne integralmente il contenuto.