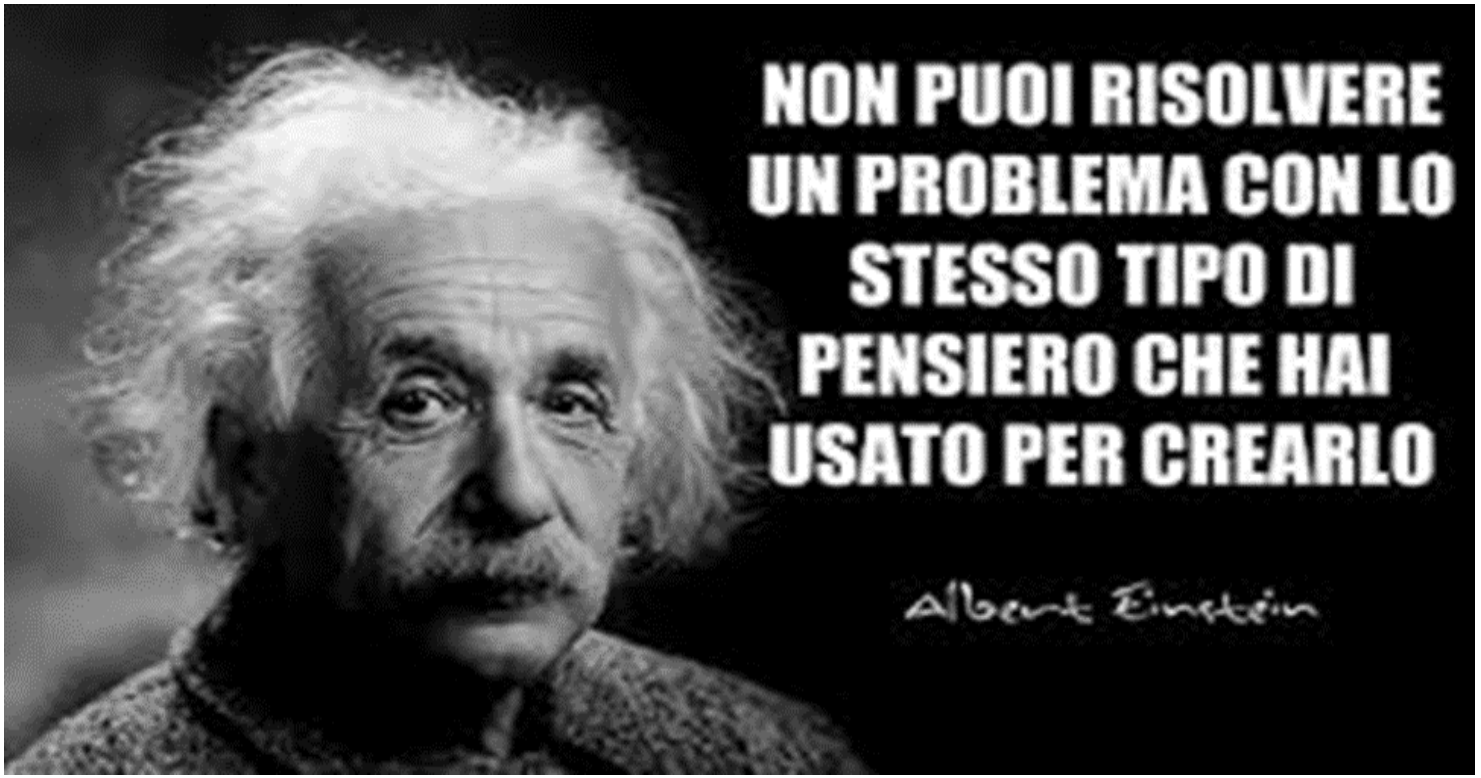
ORDINE PROVINCIALE dei Medici Chirurghi e degli Odontoiatri di MODENA

GDPR

GENERAL DATA PROTECTION REGULATION

DECRETO LEGISLATIVO 10 Agosto 2018, n. 101


NON PUOI RISOLVERE
UN PROBLEMA CON LO
STESSO TIPO DI
PENSIERO CHE HAI
USATO PER CREARLO
Albert Einstein

Il nuovo quadro normativo chiama ad un respiro molto diverso che **si articola intorno a 3 nuovi cardini (Principi)**:

il principio della "proprietà" e del controllo dei dati in capo all'interessato (considerando 7 del GDPR e art. 12-22 sui diritti dell'interessato), **il principio dell'accountability** in capo ai titolari ed ai responsabili (art. 5 - 24 GDPR) ed in generale **il principio di protezione dei dati** nell'interno dell'intero sistema (art. 32 sulla sicurezza e 33 sul data breach GDPR).

Quindi ben venga una scelta che obbliga a pensare in modo diverso: perchè questo è il vero nuovo quadro

Diritti	Come tutelare i tuoi dati

Doveri	Come trattare correttamente i dati

FERMIAMOCI UN ATTIMO è
fondamentale CAPIRE cosa dobbiamo SAPERE e cosa dobbiamo FARE

Chi sono LE PARTI IN GIOCO

Titolare del trattamento: la persona fisica o giuridica titolare del trattamento: **Tratta il dato.**

Interessato del trattamento: **la persona fisica** i cui dati sono oggetto del trattamento: **Paziente.**

Incaricato del Trattamento: la persona fisica che su direttive (formazione) del titolare tratta i dati personali (dipendente: impiegata, assistente o collaboratore interno)

Responsabile del trattamento esterno: **la persona fisica o giuridica** responsabile del trattamento (es: commercialista, consulente del lavoro)

DPO: Data Protection Office (ove necessario) **Professionista**. Una figura che ha il compito di controllare che le norme del GDPR vengano rispettate. È un **mediatore** tra l'azienda ed il Garante della Privacy.

NOVITA' del REGOLAMENTO

I TERMINI DI **CONGRUITA'** e DI **COERENZA** DIVENGONO uno STRUMENTO DI **SNELLIMENTO**

basato sul **PRINCIPIO** di:

ACCOUNTABILITY cioè **RESPONSABILIZZAZIONE**

viene affidato al titolare del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative

Fare tutto quello che è necessario. Il Titolare dovrà saper dimostrare con ragionamento Logico cosa è stato fatto e cosa non è stato fatto. Anche la scelta di non fare una determinata cosa potrà essere leggitimata, ma in ogni caso dovrà essere dimostrata.

(approccio anglosassone si tratta di una logica inversa del diritto romano)

il binomio Responsabilizzazione-Titolare del trattamento rappresenta il basamento del GDPR, una delle colonne portanti del medesimo è la coppia Informazioni-Diritti.

IL PRINCIPIO CARDINE di RESPONSABILIZZAZIONE richiede al TITOLARE DEL TRATTAMENTO DI VERIFICARE COSTANTEMENTE NEL TEMPO LA PROTEZIONE DEI DATI E LA LORO CONTINUA ADEGUATEZZA IN CONSIDERAZIONE AI CAMBIAMENTI CHE SI VERIFICANO SUL TRATTAMENTO .

Vademecum

«Regolamento UE 2016/679» - GDPR

Vuole essere un insieme di **suggerimenti**
sia di carattere **NORMATIVO** **sia** di **SEMPLICE BUONSENSO**

L' Art. 4 del GDPR introduce il termine CATEGORIE PARTICOLARI DI DATI PERSONALI
(definiti dal Codice della Privacy come «dati sensibili»)
come **qualsiasi informazione** che riguarda **SOLAMENTE LA PERSONA FISICA**

il MEDICO durante l'espletamento della propria attività professionale si trova a dover TRATTARE nei confronti **dell'INTERESSATO del TRATTAMENTO :**

- **Dati Genetici** (informazioni univoche sulla fisiologia o sulla salute della persona fisica **riguardano caratteri** generali **ereditari** che si possono individuare tramite il **DNA** (art. 4 n. 13 GDPR);

- **Dati Biometrici** (quali **l'immagine facciale** art. 4 n. 14 GDPR);

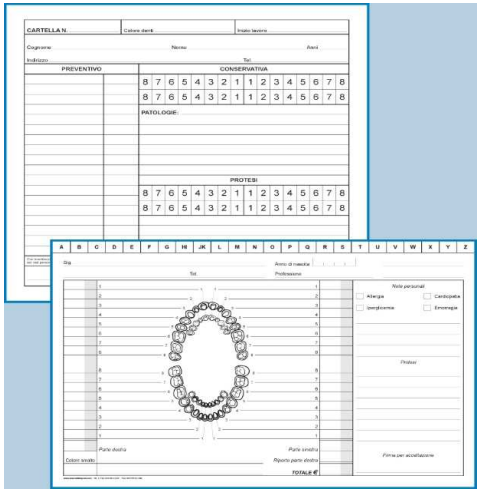
- **Dati sulla Salute** (attinenti alla salute **fisica o mentale** compresa la prestazione di servizi di assistenza sanitaria, che **rivelano informazioni** relative al suo **stato di salute** (art. 4 n. 15 GDPR)

TRATTAMENTO DEI DATI PERSONALI

PROTEZIONE DELLE PERSONE FISICHE + LORO LIBERA CIRCOLAZIONE

ALCUNI ESEMPI di **dati personali** :

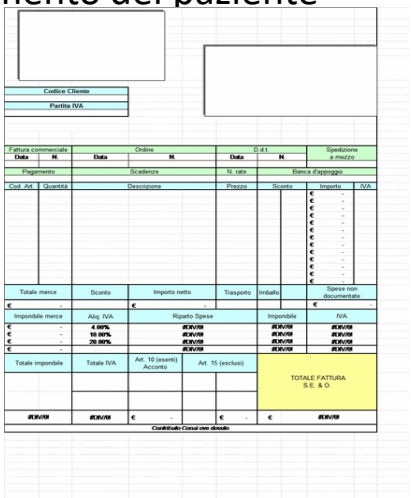
1. **Cartella Clinica** Cartacea o Informatizzata



2. **Manufatti** Protesici, Modelli , Prescrizioni

3. **Radiografie** su carta o su supporto digitale

4. **Qualunque altra informazione** presente sul **computer, registrata su dischetti**, su monitor in caso di **videosorveglianza** che possa ricondurre ai pazienti, **documenti fiscali** contabili di riconoscimento del paziente



TRATTAMENTO DEL DATO PERSONALE

Qualsiasi operazione o insieme di operazioni, compiute **con o senza** l'ausilio di **processi automatizzati** e applicate a dati personali come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, la consultazione, l'uso, la cancellazione o la distruzione (*) la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione.

(*)I distruggi documenti tre tipologie di taglio: a strisce, a frammenti o a micro-frammenti.

CONSERVAZIONE DEL DATO PERSONALE:

Nel caso in cui i dati sono conservati su **supporto cartaceo** **occorre garantirne l'accessibilità riservata** ad esempio la segretaria dello studio medico potrà avere libero accesso ai recapiti del paziente, **non** certo a quelli concernenti le condizioni di salute dello stesso; del pari, le comunicazioni telefoniche con i pazienti debbono essere effettuate in maniera che non possano essere ascoltate da soggetti terzi, estranei al rapporto.

Nel caso di **database informatico/gestionale** i files **non** debbono essere liberamente accessibili dal PC e, in ipotesi di **rete di condivisione**, sarebbe opportuno procedere ad una **pseudonomizzazione** dei dati stessi attraverso un codice identificativo che non sia, a sua volta, un dato personale del paziente.
Necessita la presenza di una **password sui terminali** mediante le quali è possibile accedere ai dati dei pazienti, e la stessa è da **cambiare ogni tre mesi.**

Il MEDICO- indipendentemente dalle dimensioni del proprio STUDIO - è TENUTO ad:

INFORMARE: ATTIVITA' DIRETTA a fornire **CONOSCENZE UTILI, IN-SEGNARE**, (**DARE NOTIZIE**)

Chi?

IL PAZIENTE (l'interessato) circa la **FINALITA'** in ragione delle quale sono **RACCOLTI I suoi DATI** nonché le **MODALITA'** di trattamento e **CONSERVAZIONE** dei dati stessi da qui la necessità di dover redigere un documento che prende il nome di

«INFORMATIVA»

A seguito della **comunicazione** e **sottoscrizione dell'Informativa** il paziente potrà prestare formalmente il proprio

«CONSENSO INFORMATO»

I DATI RACCOLTI DAL MEDICO DEVONO ESSERE…..

- **FINALIZZATI** : **strettamente pertinenti** a quanto necessario per lo scopo del trattamento dichiarato. Conseguentemente, l'informazione espressa da parte del medico delle finalità in funzione delle quali il consenso del paziente è espresso deve precedere l'acquisizione del consenso affinché quest'ultimo sia effettivamente consapevole.
- **ACCURATI** : occorre verificarne la **correttezza**, la **veridicità** e la **completezza**. Conseguentemente, il medico è tenuto **non solo a trattare dati esatti** garantendone la qualità; il medico deve anche approntare un'organizzazione che garantisca il relativo controllo, con adozione di tutte le misure necessarie alla rettificazione o **cancellazione di dati inesatti.**
- **LIMITATI** : quantitativamente determinati a quanto **strettamente necessario** alle **finalità dichiarate nell'informativa.**
- **UTILIZZATI** : in modo **riservato e confidenziale**: il medico deve garantirne la sicurezza attraverso l'utilizzo di sistemi di sicurezza (ad esempio: attraverso la cifratura dei dati: associando il dato personale relativo allo stato di salute di un assistito non direttamente al suo nominativo, ma ad un codice in base al quale individuare solo in maniera indiretta – attraverso l'accesso ad una banca dei nomi dei pazienti "cifrati", **banca dei nomi a sua volta garantita da password se telematica o da forme di sicurezza "materiali" se fisica.**
- **CONSERVATI : archiviati non oltre il tempo** strettamente necessario: il tempo necessario è quello indispensabile **alle finalità del TRATTAMENTO…**

…. e trattati in maniera:

- **LECITA** : deve fondarsi sul **consenso dell'interessato** o su altra base giuridica. Il trattamento è considerato sempre lecito se necessario all'adempimento di un obbligo legale.
- **CORRETTA** : nel **rispetto dell'informazione** resa all'interessato in relazione alla raccolta, all'utilizzo e ad altri successivi trattamenti dei dati forniti.
- **TRASPARENTE** : deve essere realizzato con modalità predefinite e rese **note all'interessato in maniera chiara, semplice ed accessibile, anche in relazione alla "forma" utilizzata. Pertanto, è da escludersi l'utilizzazione, in ambito medico, di una terminologia eccessivamente tecnica**. Prima di esprimere il proprio consenso l'interessato deve essere compiutamente informato delle modalità e delle finalità di trattamento dei dati.

IL CONSENSO deve quindi essere espresso in modo: **LIBERO – INEQUIVOCO - SPECIFICO**

Il GDPR non prevede obbligatoriamente la forma scritta per il consenso; **la forma scritta è opportuna e raccomandata**, in quanto l'art. 7 GDPR onera il titolare del trattamento di ***dimostrare*** *che l'INTERESSATO ha prestato il proprio CONSENSO al trattamento dei propri dati personali.*

Se le finalità mutano si dovrà, pertanto, acquisire un nuovo consenso.

IL CONSENSO INFORMATO
NON EQUIVALE AL CONSENSO AL TRATTAMENTO SANITARIO!

Il consenso di cui stiamo parlando ***riguarda esclusivamente*** *l'autorizzazione che il paziente dà al medico di* ***utilizzare i suoi dati personali per le finalità di diagnosi e di cura.***

Tutt'altra cosa è il ***consenso del paziente all'atto medico, che riguarda l'art. 32 della Costituzione****, a norma della quale nessuno puo' essere obbligato ad un trattamento sanitario contro la sua volontà … … …*

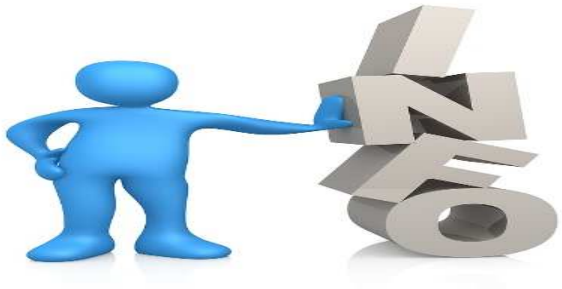
Art. 32 Costituzione Italiana

La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività, e garantisce cure gratuite agli indigenti.

Nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge. La legge non può in nessun caso violare i limiti imposti dal rispetto della persona umana.

L'INFORMATIVA (ARTT. 13 e 14 del GDPR)

E' LA NOSTRA CARTINA TORNA SOLE....



Il medico dovrà fornire con **linguaggio semplice e chiaro** le informazioni relative al trattamento dei dati devono essere in forma **concisa, trasparente,** intellegibile e facilmente accessibile e **dovrà contenere:**

- l'identità e i dati di **contatto del medico – titolare del trattamento -**(recapiti: telefono; fax; indirizzo di posta elettronica) per le comunicazioni relative all'esercizio dei diritti.

- I dati di contatto del Responsabile della protezione dei dati **DPO (ove applicabile)**

- La **precisa** e dettagliata **descrizione delle finalità** per cui viene posto in essere il trattamento. (espletare prestazioni odontoiatriche e adempimenti fiscali / amministrativi) .

- Le **Figure** preposte ad essere i **destinatari del trattamento dei dati personali** del **paziente (esempio: assistente di studio, odontotecnico, odontoiatri o medici, commercialista , tecnico software ….)**

- Il **Periodo di conservazione dei dati** personali (sotto l'aspetto medico e la tutela del paziente in relazione alle prestazioni odontoiatriche si ritiene illimitata e nel caso di inutilizzo sarà conservata nel rispetto di quanto disciplinato dall'art. 32 RGRP.

- L’intenzione del titolare del trattamento di **trasferire dati personali a paese terzo (ove applicabile)** solo quanto esistono nei confronti dei paesi garanzie adeguate di rispetto della normativa sulla privacy europea
- La specifica e **chiara indicazione dei diritti di revoca del consenso, di accesso ai dati, di rettifica**, di **cancellazione (art. 17)** di limitazione del trattamento, di **portabilità dei dati (art. 20) e di opposizione** che però varia a seconda della **motivazione**: in caso di opposizione dei dati personali non sarà poi possibile procedere con le prestazioni odontoiatriche e/o sanitaria mentre qualora i dati personali siano trattati per finalità di marketing diretto l’interessato ha diritto di opporsi in qualsiasi momento.
- Il diritto di proporre **reclamo all’Autorità di Controllo** «Garante per la protezione dei dati personali»

L’INFORMATIVA DEVE ESSERE PRESENTATA SEMPRE PRIMA DELLA PRESTAZIONE ODONTOIATRICA

Approfondiremo nelle successive slide l’argomento .....

Diritti degli interessati ai sensi degli artt. 11 e 12 del regolamento

Modalità per l'esercizio dei diritti:

• **Il termine per la risposta all'interessato** è, per tutti i diritti (compreso il diritto di accesso), **1 mese,** estendibile fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.**

• Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire **l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo** caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità;

• La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Diritto di accesso (art. 15)

• Il diritto di accesso prevede in ogni caso **il diritto di ricevere una copia** dei dati personali oggetto di trattamento.

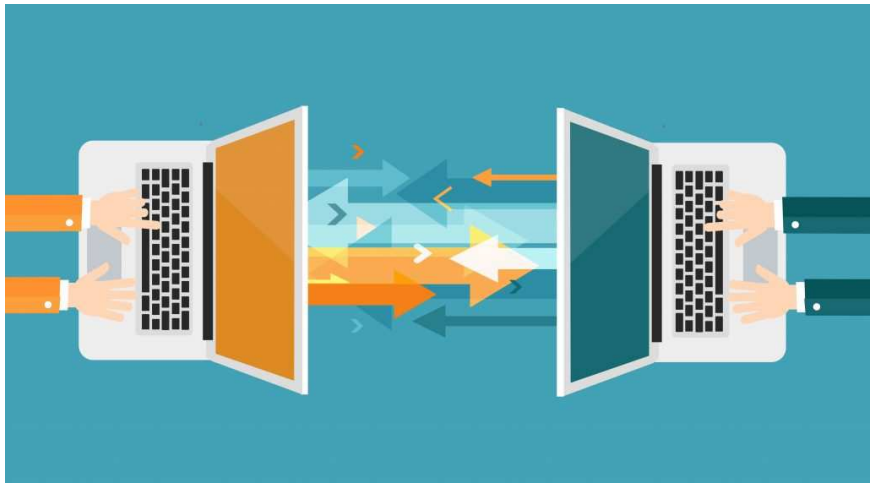
• Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi

Diritto di cancellazione (diritto all'oblio) (art.17)

• Il diritto **cosiddetto *"all'oblio" si configura come un diritto alla cancellazione dei propri dati personali*** in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di **Cancellazione** altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

- Il diritto di ottenere, in talune circostanze, la cancellazione dei dati presenti all'interno degli archivi qualora non rilevanti ai fini della prosecuzione del rapporto contrattuale o **necessari per obbligo di legge.**

• Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).



Diritto alla portabilità dei dati (art. 20)

• Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

• **Non si applica** ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare (si veda il considerando 68 per maggiori dettagli).

• Inoltre, **il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.**

Registro dei trattamenti (art. 30)

• Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio.** Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Esempio REGISTRO TRATTAMENTI…..

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI

Quali informazioni deve contenere?

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (art. 30, par. 1 del RGPD)

nel campo **"finalità del trattamento"** indicazione distinta per **tipologie di trattamento** (es. trattamento dei **dati dei dipendenti per la gestione del rapporto di lavoro**; oppure **trattamento dati per finalità di anamnesi, diagnosi, terapia sanitaria, prevenzione e riabilitazione** trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del RGPD; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018 – [doc web n. 8080493]). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2del RGPD; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del RGPD;

Nei campi **"descrizione delle categorie di interessati e delle categorie di dati personali"** andranno specificate sia le **tipologie di interessati (es. clienti, fornitori, dipendenti)** sia quelle di **dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);**

nel campo **“categorie di destinatari a cui i dati sono stati o saranno comunicati”** andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. **enti previdenziali** cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il **servizio di elaborazione delle buste paga** dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

nel campo **“trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale”** andrà riportata l’informazione relativa ai suddetti trasferimenti unitamente all’indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle “garanzie” adottate ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d’impresa, clausole contrattuali tipo, ecc.);

nel campo **“termini ultimi previsti per la cancellazione delle diverse categorie di dati”** dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. “in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall’ultima registrazione – v. art. 2220 del codice civile”). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. “in caso di contenzioso, i dati saranno cancellati al termine dello stesso”);

nel campo **“descrizione generale delle misure di sicurezza”** andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell’art. 32 del RGDP tenendo presente che l’elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l’Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l’insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (**es. procedure organizzative interne**; ecc.).

Può contenere informazioni ulteriori?

Può essere riportata nel registro qualsiasi altra informazione che il titolare ritenga utile indicare (ad es. le modalità di raccolta del consenso, l'indicazione di eventuali "referenti interni")

Quali sono le modalità di conservazione e di aggiornamento?

Il Registro dei trattamenti è ***un documento di censimento e analisi dei trattamenti*** effettuati dal titolare
Il Registro deve essere mantenuto ***costantemente aggiornato*** poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso **recare, in maniera verificabile, la data della sua prima istituzione** (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) **unitamente a quella dell'ultimo aggiornamento**. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

"- scheda creata in data XY"

"- ultimo aggiornamento avvenuto in data XY"

Misure di sicurezza (Art. 32) definite anche MISURE di GARANZIA

• Le misure di sicurezza devono **"garantire un livello di sicurezza adeguato al rischio"**

L'art 32 prevede che il TITOLARE del TRATTAMENTO e il RESPONSABILE (ove presente) **debbano adottare ed attuare delle misure tecniche organizzative che siano idonee a garantire un livello di sicurezza adeguato rispetto al rischio** che il trattamento potrebbe comportare sui diritti e le libertà delle persone fisiche interessate

MISURE TECNICHE:

-Pseudonimizzazione

Cifratura dei dati personali

-Assicurare la riservatezza, l'integrità, la disponibilità e la **resilienza (**capacità di adattarsi al cambiamento) dei servizi di trattamento

-**Capacità di ripristinare tempestivamente** l'accesso ai dati in caso di incidente tecnico

-**Procedura che possa testare**, verificare la sicurezza del trattamento

- MINIMIZZAZIONE

Le misure adottate possono essere sia TECNICHE attraverso strumenti informatici/elettronici e sia ORGANIZZATIVE è cioè affidate ai comportamenti dei soggetti che operano nella Struttura del Titolare (es: Protocolli/Procedure)

(DLGS 101/18)

ESEMPIO: LE MISURE DI GARANZIA CHE RIGUARDANO I DATI GENETICI e il TRATTAMENTO DEI DATI RELATIVI ALLA SALUTE PER FINALITA' DI PREVENZIONE, DIAGNOSI E CURA POSSONO INDIVIDUARE UN CERTO LIVELLO DI RISCHIO ecco perché il CONSENSO viene CONSIDERATA COME ULTERIORE MISURA DI PROTEZIONE DEI DIRITTI DELL'INTERESSATO.

Notifica delle violazioni di dati personali

L'Art. 33 prevede un ULTERIORE adempimento a carico del TITOLARE DEL TRATTAMENTO allorquando egli viene a conoscenza del fatto che si è verificata una situazione di c.d. **DATA BREACH**, la quale si sostanzia in un **EPISODIO DI DISTRUZIONE ACCIDENTALE O ILLEGALE DI PERDITA DI MODIFICA DI RIVELAZIONE O DI ACCESSO NON AUTORIZZATO AI DATI PERSONALI TRASMESSI CONSERVATI O COMUNQUE ELABORATI**

SI PREVEDE IN CASO DI VIOLAZIONE DEI DATI PERSONALI TRATTI CHE IL TITOLARE DEL TRATTAMENTO DEVE

A) **Notificare al GARANTE della privacy entro 72 ORE al momento in cui ne è venuto a conoscenza**
B) **Nel caso in cui detta notifica avvenga dopo le 72 ore deve essere accompagnata da una giustificazione motivata**

CONTENUTO della notifica:

- **Descrizione della Natura della violazione del dato personale**
- **Comunicare il nome e i dati di contatto del responsabile della protezione dei dati**
- **Descrizione della conseguente violazione dei dati personali**
- **Descrizione misure adottate per porre rimedio alla violazione**

Esempio di DATA BREACH

Responsabile della protezione dei dati (DPO)

• Anche la designazione di un **“responsabile della protezione dati”** (RPD, ovvero DPO se si utilizza l’acronimo inglese: Data Protection Officer)

Chi è il DPO? Il DPO è un **professionista** con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati.

Viene proposto dal titolare e dal responsabile del trattamento **in tre occasioni**:

1.quando il trattamento è effettuato da **un’autorità pubblica** o da un organismo pubblico (ad eccetto delle autorità giurisdizionali nell’esercizio delle loro funzioni);

2.**quando i trattamenti consistono e richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;

3.**quando il trattamento riguarda, su larga scala, dati sensibili o relativi a condanne penali e reati.**

La Valutazione d'Impatto sulla Protezione dei Dati. Rubricata negli artt. 35-36 GDPR

si configura come un'autonoma valutazione che il Titolare del trattamento pone in essere per analizzare la necessità, la proporzionalità e i rischi di un determinato trattamento dati per i diritti e le libertà delle persone fisiche. È richiesta in particolar modo in tre casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il **trattamento, su larga scala,** di **categorie particolari di dati personali** di cui all'articolo 9,

paragrafo 1, o di dati relativi a **condanne penali e a reati** di cui all'articolo 10; o

c) la **sorveglianza sistematica** su larga scala di una zona accessibile al pubblico (es. **Videosorveglianza su larga scala).**

Ora, la parte che potrebbe interessare maggiormente uno Studio medico e odontoiatrico è il b). Entrando "a gamba tesa" con la parte finale del **considerando 91 GDPR** si può affermare che **"Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati."**

Ma volendo occuparci non del singolo medico ma di più medici (nel singolo studio o in studi associati), cosa significa trattamento su larga scala? **Secondo le Linee Guida** del già "Gruppo dei Garanti Privacy europei" (WP29)[19],[20] **per determinare se un trattamento è svolto su larga scala si deve far riferimento al numero degli interessati, al volume di dati e/o tipologie di dati, alla durata dell'attività di trattamento e all'ambito geografico dell'attività di trattamento. In parole povere, se lo Studio tratta dati particolari su larga scala, è tenuto a porre in essere una Valutazione d'Impatto.**

Cosa deve contenere la Valutazione d'Impatto?

Ora, ammesso **che è difficile che la maggior parte degli Studi medici e odontoiatrici tratti dati particolari su larga scala (prerogativa di un ospedale, ad esempio),** vediamo **cosa deve** essere presente in una Valutazione d'Impatto a norma di legge. L'art. 35.7 dispone che la Valutazione d'Impatto deve **contenere**:

una **descrizione sistematica dei trattamenti** previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

una **valutazione** della necessità e proporzionalità **dei trattamenti in relazione alle finalità;**

una **valutazione dei rischi per i diritti e le libertà degli interessati** di cui al paragrafo 1; e

le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza **e** i meccanismi per **garantire la protezione dei dati personali** e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Tutto questo da realizzare avvalersi di un software

DOMANDE sul GDPR

cosa deve fare il medico nel suo studio per essere in regola con la privacy dopo l'entrata in vigore del Regolamento Europeo 679/2016? Ci sono alcuni **adempimenti** che il medico è tenuto a fare per ottemperare alle norme del Regolamento Europeo, che si possono riassumere così:

- **identificare i soggetti interessati** al trattamento dei dati;
- predisporre un'adeguata **informativa**;
- raccogliere il **consenso;**
- istituire il **Registro dei trattamenti** dei dati;
- elaborare **procedure** per **fronteggiare** le ipotesi di **violazione** della privacy
- **Formazione** personale (incaricati)

Cominciamo dal primo punto: identificare i **soggetti interessati**. **Chi sono?** Secondo logica, i soggetti interessati al trattamento dei dati da parte di un medico sono i suoi **pazienti**. **Ma non solo**: il medico potrebbe gestire anche i dati personali del suo **personale dipendente** o dei suoi **collaboratori**. Infine il medico potrebbe dover avere necessità di gestire anche i dati personali di soggetti che non sono né suoi pazienti né suoi dipendenti o collaboratori. Ad esempio i **fornitori**.

Questo primo passo da fare serve per calibrare poi i successivi adempimenti.

……RIPRENDIAMO IL CONCETTO DELL'INFORMATIVA…..

INFORMATIVA

Cos'è l'informativa sul trattamento dei dati personali? È una **dichiarazione scritta** con linguaggio **semplice e chiaro** da rendere nota al paziente anticipatamente rispetto al trattamento dei dati da redigere in **forma concisa, trasparente, intellegibile e facilmente accessibile**. Necessaria per ogni singolo paziente e affissa nella sala d'attesa dello studio in modo da **renderla conoscibile** alla generalità degli utenti dello studio. **L'informativa deve contenere tutta una serie di informazioni**, secondo quanto previsto dal Regolamento Europeo, che si possono così **riassumere**:

- **dati di contatto del Titolare** dello Studio;
- **dati di contatto del Responsabile del trattamento dei dati** (ove esistente);
- **dati di contatto** del Responsabile della protezione dei dati – **DPO** (ove esistente);
- **finalità e scopo** del trattamento dei dati;
- **modalità** di trattamento dei dati e raccolta consenso;
- **tempo di conservazione** dei dati;
- **soggetti a cui i dati vengono comunicati**;
- **trasferimento all'estero dei dati**;
- **diritti dell'interessato**.

E' importante ricordare che **l'informativa è un adempimento obbligatorio** e in nessun modo eludibile

Entriamo nel vivo dell'informativa:

In primo luogo l'informativa deve contenere i **dati di contatto del Titolare dello studio (nominativo, sede, telefono, email).** Se il titolare dello studio nomina un responsabile del trattamento dei dati, deve indicare gli stessi dati anche per il responsabile. La nomina di tale responsabile non è obbligatoria. Se il titolare dello studio nomina un responsabile per la protezione dei dati (DPO), deve indicare gli stessi dati anche per il DPO (ove necessita).

Finalità e Scopi del trattamento Vanno indicate **le finalità** del trattamento e **lo scopo per cui si raccolgono, si gestiscono e si trattano i dati dei pazienti.**

La **finalità** principale per uno **studio medico è: prevenzione, diagnosi, cura, riabilitazione o per a ltre prestazioni di natura medica o sanitaria richieste dal diretto interessato, anche farmaceutiche o specialistiche** . Ci sono poi **altre finalità**, che sono obbligatorie per legge, **ad esempio Comunicare i dati a soggetti, enti o autorità a cui la comunicazione sia obbligatoria in forza di disposizioni di legge o ordini delle autorità .** Oppure le **finalità** possono derivare da precisi rapporti contrattuali, come ad esempio **nel caso di pazienti che aderiscono a fondi mutualistici o a polizze assicurative**. In questi casi la **finalità** dello studio medico è anche **quella di comunicare i dati ad enti privati per motivi assicurativi su richiesta dell'interessato.** Un'altra importante **finalità** per cui lo studio medico tratta i dati dei propri pazienti esercitare i diritti legali del titolare dello studio, ad esempio il **diritto di difesa in giudizio** . Solitamente questi sono gli scopi e le finalità che ogni studio medico si prefigge nel trattare i dati dei propri pazienti, per cui si può dire che quanto sopra rappresenta l'informativa "minimale" riguardo alle finalità del trattamento. Se il titolare dello studio, avendo riguardo alla sua specifica attività medica, si rende conto che utilizza i dati dei pazienti anche per altri e ulteriori scopi, deve dichiararlo esplicitamente nell'informativa che quindi va adeguatamente integrata.

Quali possono essere altre FINALITA' di trattamento? Ad esempio condurre **attività di ricerca scientifica** o epidemiologica, utilizzare i dati dei pazienti per pubblicazioni scientifiche o presentazioni ai congressi, **spedire una periodica newsletter ai pazienti per informarli sulle attività dello studio**. Sono tutte **finalità ulteriori** rispetto a quella fondamentale di attività assistenziale che quindi **vanno separatamente evidenziate** per **renderle note al paziente**.

MODALITA' di trattamento dei dati Il **titolare** dello studio **deve dichiarare che si ispira ai principi di LICEITA', correttezza, trasparenza, minimizzazione e limitazione dei dati**, come previsto dal Regolamento Europeo. Una formula utilizzabile potrebbe essere la seguente: **I dati potranno essere trattati in forma cartacea ed elettronica**, con **accesso consentito** ai soli operatori autorizzati, precedentemente nominati (definiti ad esempio: addetti al trattamento) i quali seguono corsi di formazione specifici e vengono periodicamente aggiornati sulle regole della privacy e sensibilizzati al rispetto e alla tutela della dignità e della riservatezza del paziente. **Tutti gli operatori dello Studio che accedono ai dati informatizzati sono identificabili e dotati di password personale; l'accesso ai dati è consentito solo per le finalità legate al ruolo dell'operatore e solo per lo stretto tempo necessario a trattare la prestazione** per la quale il paziente si è recato presso lo Studio.
Lo Studio non svolge attività di profilazione dei dati dei propri assistiti.

TEMPO di conservazione dei dati **Nell'informativa va anche indicato il tempo di conservazione dei dati** da parte dello studio. Intanto una formulazione adeguata nell'informativa potrebbe essere la seguente: **I dati personali e sensibili verranno conservati per il tempo previsto dall'attuale normativa**: **in particolare, i dati relativi a ciascun episodio assistenziale, raccolti nella relativa scheda sanitaria, verranno conservati a tempo indeterminato, perdurando il rapporto contrattuale di cura. Al termine del rapporto contrattuale di cura, lo Studio conserverà i dati per un periodo non superiore al termine prescrizionale di legge per la tutela dei propri diritti legali e di difesa.**

Non si applica il diritto alla cancellazione nell'ambito dello Studio medico e odontoiatrico quando:

- vi è un obbligo di legge da rispettare, un compito da svolgere nel pubblico interesse ovvero l'esercizio di pubblici poteri cui può essere investito lo Studio;
- non si applica quando vi sono motivi di interesse pubblico nel settore della sanità pubblica (es. trattamento necessario per finalità di medicina preventiva, medicina del lavoro, diagnosi, assistenza, terapia sanitaria ecc.);
- non si applica per fini di archiviazione nel pubblico interesse e ricerca scientifica nella misura in cui il diritto alla cancellazione non pregiudichi tali obiettivi;

ed infine

- non si applica per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria (art. 24 Cost.).

Comunicazioni A TERZI dei dati Una formulazione suggerita può essere la seguente: **I dati non verranno in alcun modo diffusi, ma potranno essere trasmessi agli Enti competenti per finalità amministrative** istituzionali, secondo quanto richiesto dalla normativa vigente.

Piu' precisamente **i dati potranno essere comunicati a destinatari appartenenti alle seguenti categorie**:

- soggetti interni allo Studio con funzione di **Incaricati al trattamento;**
- **professionisti medici e personale sanitario**, anche **con rapporto di collaborazione** occasionale con lo **Studio**;
- soggetti esterni incaricati di funzioni di manutenzione e assistenza dei sistemi informatici e di comunicazione;
- soggetti esterni consulenti in materia fiscale;
- Autorità ed Enti Pubblici competenti per obbligo di legge;
- (eventuali altre categorie di destinatari).

I soggetti appartenenti alle categorie suddette svolgono la funzione di Responsabile del trattamento dei dati, oppure operano in totale autonomia come distinti Titolari del trattamento. **I dati potranno essere comunicati a familiari o conoscenti solo su espressa autorizzazione dell'interessato.**

TRASFERIMENTO all'ESTERO dei dati **Di norma uno studio medico non ha mai necessità di trasferire all'estero** i dati dei propri pazienti.

Però bisogna aver presente che lo studio **può avvalersi di strumenti informatici che si "appoggiano" su server ubicati al di fuori del territorio italiano.**

Per cui una formulazione suggerita può essere la seguente: **I dati personali sono conservati su server ubicati all'interno dell'Unione Europea.**

DIRITTI dell'interessato

In questa sezione dell'informativa occorre riportare i diritti dell'interessato

Ai sensi dell'art . 15 del GDPR, **l'interessato ha il diritto** di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, **di ottenere l'accesso ai dati personali e alle seguenti informazioni:**

a) **le finalità** del trattamento;
b) **le categorie dei dati** in questione;
c) **i destinatari** o le categorie di destinatari **a cui i dati** personali sono stati o **saranno comunicati**;
d) **il periodo di conservazione** dei dati personali previsto oppure dei criteri determinati per determinare tale periodo;
e) richiedere al Titolare l'accesso ai dati, **la rettifica o la cancellazione** dei dati personali o la **limitazione del trattamento** dei dati personali che La riguardano o di **opporsi al loro trattamento**;
f) con riferimento all'eventuale consenso prestato, il **diritto di revocare**, in ogni momento, il **consenso prestato**;
g) il diritto di proporre **reclamo all'Autorità Garante**
h) il **diritto alla portabilità** dei dati. Il diritto di ottenere il trasferimento dei dati in favore di un diverso titolare

L'interessato puo' esercitare Il **diritto all'oscuramento** dei dati (**dossier sanitario**) e cioè l'interessato puo' richiedere che alcuni dei **dati o** dei **documenti sanitari** di cui si puo' prendere visione attraverso il dossier sanitario **vengano resi non consultabili** da parte di coloro i quali hanno diritto ad accedere al fascicolo sanitario medesimo. Il **Titolare però è obbligato ad informare coloro i quali sono abilitati ad accedere ai dossier che vi è la possibilità che tali documenti siano incompleti** qualora l'interessato abbia esercitato o eserciti il diritto all'oscuramento. Le e che ha raccolto o ha elaborato i dati. **informazioni sanitarie oscurate saranno comunque sempre disponibili ed accessibili al professionista o struttura/reparto che era titolare del trattamento**

Ma se il paziente ha diritto a ottenere "la cancellazione dei suoi dati", come fa il medico a difendersi in caso di contenzioso? Il diritto alla cancellazione va messo in relazione al diritto del medico di tutelare i suoi interessi legali, per cui se il paziente chiede la cancellazione dei suoi dati prima che siano decorsi i termini di prescrizione legali, il medico può legittimamente rifiutare tale cancellazione, motivando tale decisione con la necessità di tutelare il suo diritto di difesa. Viceversa, se i termini sono oramai decorsi, il medico può tranquillamente procedere alla cancellazione, accogliendo la richiesta del paziente. In altre parole, **il "diritto all'oblio" non è assoluto: trova un limite nel diritto del medico a tutelare i suoi diritti legali.**

E cosa significa che il paziente può "revocare il consenso"? Senza di quello non può più essere curato….. Se il paziente revoca il suo consenso al trattamento dei dati per le finalità di prevenzione, diagnosi e cura, il medico non può più legittimamente averlo in cura.
Per cui, fermo restando il principio di tutela in casi di emergenza, il rapporto assistenziale è da intendersi terminato.

Cosa significa la "portabilità dei dati"? Significa che **il paziente ha diritto ad ottenere i dati che lo riguardano in un formato facilmente accessibile e gestibile con sistemi informatici.** Quindi il **paziente ha diritto a chiedere che lo studio medico gli fornisca i suoi dati o in forma cartacea o in forma digitale (in un formato facilmente accessibile).** Se il paziente lo richiede, lo studio deve essere in grado di trasmettere i dati ad un altro studio medico indicato dal paziente stesso. E anche in questo caso il formato di trasmissione deve assicurare la facilità di accesso e di interscambio.

CONSENSO

Una volta che il paziente è stato informato, cosa deve fare il medico?

Deve raccogliere il consenso. Il consenso può essere raccolto anche in forma orale, ma per evitare future ed eventuali contestazioni è opportuno che venga raccolto in forma scritta, con la sottoscrizione di un apposito modulo, anche redatto in calce all'informativa.

Se lo studio intende utilizzare i dati per finalità diverse e ulteriori rispetto a quelle meramente assistenziali (ad esempio: per sperimentazione scientifica oppure per pubblicare i dati del paziente su riviste medico-scientifiche o presentazioni a congressi oppure per inviare newsletter periodiche informative) sono necessari ulteriori e differenziati consensi.

Questo **consenso firmato dal paziente è "una tantum" o va rinnovato periodicamente? Il consenso del paziente resta valido a tempo indeterminato.**

Chi può esprimere il consenso? Solo il diretto interessato? **Generalmente sì.** Il paziente maggiorenne, capace di intendere e di volere, è l'unico soggetto autorizzato a dare il consenso per il trattamento dei propri dati sanitari. Se il paziente invece è minorenne o non è capace di intendere e di volere, allora il consenso deve essere dato rispettivamente dai genitori (anche disgiuntamente) o da chi esercita la potestà genitoriale o dal tutore.

A proposito dei minorenni: c'è qualche differenza se i genitori sono sposati o separati o divorziati? **No, nessuna differenza**. Entrambi i genitori, indipendentemente dal loro status giuridico, hanno il dovere di tutelare la salute dei propri figli, per cui hanno il diritto-dovere di essere informati sullo stato di salute dei figli e il medico deve portare a loro conoscenza i dati sanitari di cui dispone, o disgiuntamente o congiuntamente. **È responsabilità dei genitori (e non del medico) relazionarsi fra loro.**

Il consenso di cui stiamo parlando equivale al consenso al trattamento sanitario? **Assolutamente no.** Il consenso di cui stiamo parlando riguarda esclusivamente l'autorizzazione che il paziente dà al medico al trattamento dei dati ai fini della privacy. Tutt'altra cosa è il consenso del paziente all'atto medico, che non riguarda la legge sulla privacy (gdpr), **bensì l'art. 32 della Costituzione**, a norma del quale **nessuno può essere obbligato ad un trattamento sanitario contro la sua volontà**. Adesso ci stiamo occupando solo e soltanto del consenso ai fini della legge sulla privacy (gdpr).

E se il consenso viene revocato? **se il paziente revoca il suo consenso al trattamento dei dati per finalità di prevenzione, diagnosi e cura, il rapporto assistenziale non può proseguire e quindi è da ritenersi concluso** (**fatte salve le situazioni di emergenza**). Se invece il paziente revoca il consenso per finalità diverse (ad esempio, non vuole più ricevere le newsletter dallo studio), **il rapporto assistenziale prosegue** normalmente e si interrompe solo il trattamento dei dati per la specifica finalità per la quale il consenso è stato revocato.

Come garantire la sicurezza dei dati personali dei pazienti? Il GDPR su questo non fa sconti. Innanzitutto, bisogna dimenticare la coppia misure minime / misure idonee di cui al vecchio Codice. Con il GPDR le uniche misure di sicurezza ammesse sono quelle "adeguate".

L'art. 32 GDPR dispone che per approntare delle adeguate misure di sicurezza bisogna tener conto dello stato dell'arte (avanzamento tecnologico), dei costi di attuazione (delle misure di sicurezza), della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (porre in essere, quindi, un'analisi del rischio sui dati personali trattati). Il tutto per garantire un livello di sicurezza adeguato al rischio. Tra le "soluzioni" che l'art. 32 elenca – in maniera non esaustiva – vi sono:

la pseudonimizzazione e la cifratura dei dati personali;

la capacità di **assicurare su base permanente la riservatezza**, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (ovvero, anche la capacità del sistema di resistere e reagire);

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (es. **backup**);

una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche** e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Inoltre, punto importante, lo Studio Titolare del trattamento fa sì che chiunque agisca sotto la Sua autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso

È sempre utile rammentare quelle che sono le misure imprescindibili per uno Studio medico e odontoiatrico che, in un certo senso, precedono quanto previsto dall'art. 32 GDPR:

Controllo degli accessi alle postazioni PC, nonché ad altri terminali, **mediante username e password per ogni singolo operatore;**

Username e password devono essere perfettamente memorizzati, non vanno scritti su carta e collocati a vista presso la postazione PC, sono personali e non cedibili a nessuno;

Ogni volta che si abbandona la postazione PC, anche per pochi secondi, va effettuata la disconnessione dal terminale (ad esempio, Logo Windows + L);

La password va cambiata periodicamente e non oltre 90 giorni;

Su ogni PC e terminale vanno installati Antivirus e Firewall e devono essere aggiornati (preferibilmente, non affidarsi a software gratuiti);

Dotarsi di soluzioni di crittografia / pseudonimizzazione per gli archivi elettronici;

Porre in essere **backup periodici** e replicare le stesse misure di sicurezza sui terminali mobili (smartphone, tablet ecc.).

FORMALIZZAZIONE DEI RUOLI

Oltre a formulare l'informativa e raccogliere il consenso, cos'altro deve fare il medico nel suo studio? Se il medico, nel proprio studio, si avvale di personale di **segreteria**, deve redigere una formale lettera al personale di segreteria, che si deve attenere alle istruzioni impartite dal medico titolare dello studio.
Vedremo in seguito il fac-simile della Lettera di Incarico

Se il medico si avvale di collaboratori medici o personale infermieristico? Se il medico, nel proprio studio, si avvale di collaboratori medici o personale infermieristico, deve redigere una formale incarico
Vedremo in seguito il fac-simile della Lettera di Incarico

Se il medico si avvale di un ragioniere e/o commercialista per la tenuta della sua contabilità? Anche in questo caso va affidata al commercialista la formale responsabilità per il trattamento dei dati. Si può utilizzare il seguente modello di lettera: NOMINA QUALE RESPONSABILE ESTERNO AL TRATTAMENTO DEI DATI
Vedremo in seguito il fac-simile della Lettera di Nomina

E se lo studio è composto da più medici in forma associativa? **Se i dati dei pazienti sono condivisi da più medici** in forma stabile e continuativa**, fermo restando che ciascun medico è titolare dei dati dei suoi diretti assistiti,** necessario **sottoscrivere un accordo di contitolarità per legittimare il trattamento in comune dei dati.** Ovviamente si tratta di una situazione che va esplicitata nell'informativa e che renderà necessario approntare misure di sicurezza adeguate.

REGISTRO DEI TRATTAMENTI

Cos'è in pratica? E' un registro in cui si elencano le tipologie di trattamenti che vengono svolti dallo studio e che coinvolgono i dati personali degli interessati. Può essere realizzato in forma scritta su supporto cartaceo o elettronico.

In che cosa consiste? Si tratta di un documento conservato dove il professionista svolge l'attività. Ogni professionista deve esplicitare chiaramente da chi e come saranno trattati i dati, **dall'informativa all'archiviazione**, ma non va visto come un mero adempimento burocratico, bensì parte integrante di un sistema di corretta gestione dei dati personali, in quanto finalizzato a tenere sotto controllo il ciclo vitale del dato. E' un documento da esibire agli organi di controllo in caso di verifiche o accertamenti.

E' obbligatorio per tutti gli studi medici? Siccome gli studi medici trattano dati inerenti la salute dei propri assistiti, che sono dati particolarmente delicati e sensibili, al di là dell'esistenza di uno specifico obbligo è **fortemente raccomandato** approntare il registro, come previsto dall'art. 30 del Regolamento Europeo.

Cosa deve essere riportato sul registro? **devono essere annotati**:

- **Identificativi del titolare dello studio** e del responsabile (ove presente);
- **la Tipologia del trattamento** (ad esempio: **prestazione sanitaria**);
- **la Finalità del trattamento** (ad esempio: **rapporto di cura**) e la **base giuridica** su cui si fonda il trattamento (ad esempio: **obbligo legale oppure consenso dell'interessato**)
- **Le Categorie di soggetti interessati** (ad esempio: **pazienti**);
- **Le Categorie di dati personali trattati** (ad esempio: **dati relativi alla salute**);
- **Le categorie di Destinatari a cui i dati possono o devono essere comunicati** (ad esempio**: ASL, INPS, INAIL, Agenzia delle Entrate, Autorità Giudiziaria, Compagnie Assicurative, ecc.**) e **Responsabili Esterni** (ad esempio: il **commercialista** o il consulente del lavoro);
- i **Paesi stranieri verso cui i dati possono essere trasferiti** (ad esempio: **nessuno**);

- il **periodo di conservazione dei dati** (ad esempio: 10 anni o comunque per il tempo necessario a tutelare i diritti legali del titolare – criterio di necessità);
- **le Misure di Sicurezza** fisiche, organizzative ed informatiche adottate per la protezione dei dati; il software informatico utilizzato per il trattamento dei dati

Il registro dei trattamenti è uno soltanto? Dipende dall'organizzazione dello studio medico. Nello studio mono professionale è sufficiente la predisposizione di un solo registro dei trattamenti a cura del titolare dello studio. In altri contesti operativi potrebbe essere necessaria la predisposizione di un registro dei trattamenti per il titolare e uno per il responsabile del trattamento dei dati.

POLITICHE DI SICUREZZA

Dopo aver scritto l'informativa, fatto firmare i consensi e compilato il Registro dei trattamenti sono finiti gli adempimenti?
Da questo momento in poi **scatta la** parte **"sicurezza dei dati"** nel senso che gli adempimenti che vi ho illustrato fino ad ora avviano un processo di protezione e tutela nel trattamento dei dati perché, secondo **il Regolamento Europeo, chi gestisce i dati deve agire sul principio della "responsabilizzazione"**
Fin dall'inizio bisogna configurare il trattamento dei dati prevedendo le garanzie indispensabili per soddisfare i requisiti del Regolamento Europeo e tutelare i diritti degli interessati.
Ad esempio i **produttori di software** informatico gestionale per gli studi medici sono tenuti a ripensare i loro prodotti preoccupandosi della tutela della privacy fin dalla progettazione del software che dev'essere conforme al Regolamento Europeo **"by default".** Allo stesso modo **il medico nel suo studio** deve orientare la propria **organizzazione di lavoro in modo sempre assolutamente attento alla tutela della riservatezza dei dati dei pazienti fin dall'origine**, evitando comportamenti o prassi che mettano a rischio i diritti e le libertà personali degli interessati. Ad esempio, **deve essere valorizzata e costantemente adeguata la formazione del personale di segreteria, che deve essere consapevole dei comportamenti più adeguati a tutela della privacy. Tutto questo deve avvenire costantemente e deve sostanziarsi in una serie di attività specifiche e dimostrabili, con monitoraggi periodici.**

Il termine "Data Breach". Cosa significa? Il termine indica ogni **"violazione dei dati"** e nella pratica può significare ad esempio il **furto, la perdita, l'alterazione, la manipolazione di dati cartacei o informatici**. In questi casi **il titolare** dello studio **deve notificare** il fatto all'Autorità Garante per la privacy entro **72 ore** **dal momento in cui ne è venuto a conoscenza attraverso apposito modulo .**

Quali accorgimenti deve adottare il medico che non utilizza il computer, ma conserva tutto su carta?

Nel caso di trattamento dei dati in **forma cartacea**, il medico che istituisce le **schede sanitarie** per ogni singolo paziente **nelle quali conservare il modulo di consenso firmato e ogni altro atto e documento inerente la salute del paziente**. Le schede dovrebbero essere conservate in un luogo e in un modo tale da evitare che persone non autorizzate ne possano prendere conoscenza. Per esempio, **se sono riposte in un armadio, questo dovrebbe essere chiuso a chiave e collocato in una stanza dello studio non accessibile al pubblico in generale. Le chiavi dell'armadio dovrebbero essere in possesso solo del medico e del suo sostituto (o dei suoi collaboratori medici) e non di altre persone. Inoltre l'armadio dovrebbe essere di materiale ignifugo, in modo da evitare il rischio di perdita o distruzione di dati a causa di incendio.**

E se il medico utilizza anche il computer?

Vale lo stesso principio di evitare o ridurre al minimo il rischio di perdita, distruzione, sottrazione, manomissione o alterazione dei dati memorizzati nel computer. Ciò si può realizzare con diversi accorgimenti tecnici. In primo luogo il **computer deve essere protetto da una password alfanumerica (la meno intuitiva possibile**) che deve essere **cambiata ogni tre mesi**. Inoltre il **computer deve essere protetto da un software antivirus,** anti-malware e, **se è connesso a internet, anche da un firewall di ultima generazione, capace di identificare le minacce e bloccarle prima che si concretizzino.** Infine **deve essere previsto un salvataggio periodico dei dati** da poter utilizzare in caso di emergenza. Le misure di protezione informatica hanno una rapida evoluzione tecnologica, per cui è assolutamente necessario che il medico possa contare su un consulente informatico di propria fiducia per rendere il suo sistema sempre protetto al massimo grado.

Il collaboratore medico può usare il computer del medico titolare?

il collaboratore medico **può accedere ai fascicoli cartacei dei pazienti**, **può** certamente **accedere ai dati sanitari memorizzati nel computer** dello studio. Però è necessario che vi acceda **con un proprio nome utente e una propria password**, in modo che sul computer **rimanga una "traccia informatica" di chi, come e quando ha acceduto al sistema.** A monte ci deve essere una formale lettera di incarico.

Il personale di segreteria? Può accedere al computer e alle schede dei pazienti?

Il personale di segreteria deve limitare l'accesso solo ai dati necessari per svolgere il proprio lavoro, per cui **potrà** sicuramente **accedere ai dati personali dei pazienti come ad esempio l'indirizzo e il numero di telefono, ma non ha titolo per accedere ai dati sanitari** dei pazienti. Anche in questo caso è necessario che **l'accesso al computer sia effettuato con un nome utente e una password dedicata al personale di segreteria,** in modo che il sistema limiti automaticamente l'accesso ai dati comuni e non a quelli sensibili. A monte ci deve essere una formale lettera di attribuzione dell'incarico.

Ma il "Documento Programmatico per la sicurezza" (DPS) esiste sempre? **Il DPS deve ritenersi superato** dal Regolamento Europeo che non parla più di "misure minime di sicurezza", ma obbliga il titolare a pensare alla sicurezza al massimo grado. In pratica col **Regolamento Europeo** non bisogna limitarsi ad adottare misure di sicurezza minime, ma all'opposto bisogna approntare le procedure che diano il massimo di garanzie tecnicamente possibili per tutelare e proteggere i dati. Ed in effetti: **costruire per bene l'informativa, redigere correttamente il Registro dei Trattamenti e monitorare costantemente le proprie procedure per evitare i rischi di Data Breach** sono tutte azioni che rientrano nell'ottica della **tutela della riservatezza "al massimo grado" possibile, sia in termini di sicurezza fisica (luoghi e ambienti) che organizzativa (procedure e incarichi) che informatica (strumenti hardware e software adeguati).**

In definitiva, è preferibile usare il cartaceo o il computer? E' una scelta che dipende esclusivamente dalle modalità organizzative del singolo medico.
Se si lavora solo su carta, dovranno essere adottati alcuni accorgimenti; se si lavora col computer, altri. Si può solo dire che nella fase attuale di progresso tecnologico, l'uso del computer è sempre più utile e semplifica notevolmente il lavoro, purché ovviamente venga utilizzato con criterio e diligenza.

IL DPO

Parliamo adesso del DPO: chi è? Il Regolamento Europeo ha introdotto la figura del "Responsabile della Protezione dei Dati" (in italiano RPD e in inglese DPO). Si tratta di un soggetto, persona fisica o giuridica, **nominato dal titolare con il compito di collaborare con lui nella protezione dei dati** e che quindi può affiancare il titolare anche nella redazione dell'informativa, nella gestione del Registro dei Trattamenti, nell'elaborazione delle procedure di emergenza e nel monitoraggio costante e continuativo delle prassi all'interno dello studio. **Il DPO funge anche da punto di contatto con l'Autorità Garante per la Privacy ed è per questo motivo che il suo nominativo va comunicato al Garante.**

SUGGERIMENTI PRATICI

Il paziente ha diritto di chiedere al medico solo una copia degli atti o può pretendere di ottenere gli originali? Come già detto sopra, il paziente ha diritto alla "portabilità dei dati". Questo non significa che il medico si deve necessariamente privare dei dati per darli al paziente. Bisogna distinguere: se il paziente a suo tempo ha consegnato al medico un documento sanitario (ad esempio una radiografia) e poi successivamente chiede che gli venga restituita, il medico deve consegnare lo stesso originale che aveva ricevuto dal paziente stesso (facendosi firmare una ricevuta di consegna). Se invece il paziente chiede la propria scheda sanitaria, può ottenerne una stampa o una fotocopia o in formato digitale facilmente accessibile.

E se la richiesta proviene da un familiare o da un conoscente del paziente? Dipende se il paziente ha dato il suo consenso. Se è così, allora il medico è autorizzato a fornire i dati sanitari ai familiari o conoscenti individuati dal paziente stesso. Ma se non è così il medico non può rivelare alcunché a nessun soggetto diverso dal diretto interessato. Per evitare contestazioni, è opportuno che il medico si faccia indicare per iscritto chi sono i soggetti a cui acconsente che siano forniti dati e/o informazioni sul suo stato di salute.

La consegna di documenti sanitari (ad esempio un certificato medico o una ricetta) deve farla materialmente il medico o può farlo anche il personale di segreteria? Può farlo anche il personale di segreteria, ma in tal caso il documento sanitario deve sempre essere chiuso in una busta e spetterà al personale di segreteria identificare il soggetto che ritira la busta: se il diretto interessato o se un delegato. In quest'ultima ipotesi, dovrà acquisire la delega del diretto interessato.

La delega al familiare o al conoscente deve essere rinnovata volta per volta? Il paziente può liberamente decidere di dare una delega in forma scritta per il ritiro di un singolo documento che lo riguarda.

Le buste chiuse contenenti i documenti sanitari possono essere messe a disposizione dei pazienti per il ritiro, ad esempio in uno scaffale della sala d'attesa dello studio? No, perché così facendo non si sa chi è il soggetto che ritira la busta e potrebbe anche succedere che il paziente (magari anche in buona fede) ritiri una busta che non è la sua. Per evitare questi rischi di indebita conoscenza di dati sanitari da parte di terzi non autorizzati, una efficace misura di sicurezza, ad esempio, è inserire le buste in appositi schedari ubicati non nella sala d'attesa dello studio, bensì nello spazio dedicato alla segreteria. In questo modo l'identificazione del soggetto e la consegna della busta è mediata dal personale di segreteria, che deve attenersi alle regole di tutela della privacy - Gdpr.

Se il paziente chiede al medico una attestazione dettagliata del suo stato di salute, perché per esempio deve presentarla al datore di lavoro per usufruire di permessi speciali, o alla compagnia di assicurazione per un risarcimento, il medico può rifiutarsi di farlo per motivi di privacy? Assolutamente no. La decisione se rivelare al datore di lavoro o ad altri soggetti i dati inerenti lo stato di salute spetta al paziente, non al medico. Quindi se il paziente desidera ottenere dei permessi speciali o benefici assicurativi e vuole giustificare questa richiesta con una certificazione medica dettagliata, il medico deve soddisfare la richiesta del suo assistito, dichiarando i dati sanitari in suo possesso-

E se la richiesta di dati e informazioni sanitarie proviene da un qualunque altro soggetto? In generale vale la regola per cui senza il consenso del diretto interessato, il medico non può comunicare niente a nessuno. Quindi, solo se c'è il consenso del paziente il medico può fornire dati e informazioni sanitarie ad altri soggetti, come ad esempio alla compagnia di assicurazione del paziente, al datore di lavoro del paziente, e così via.

Ci sono casi in cui il medico è autorizzato a comunicare a terzi i dati sanitari del paziente, in assenza del suo consenso? Sì, ma sono previsti da specifiche norme di legge (nazionali o regionali) e ciò deve già risultare dall'informativa, come detto sopra. Per esempio nei casi in cui sussiste obbligo di referto, il medico è tenuto a segnalare all'autorità giudiziaria i dati in suo possesso anche senza il consenso del diretto interessato. Oppure per la segnalazione di malattie infettive o diffusive. Così come i medici convenzionati (medici di famiglia e pediatri) sono tenuti a comunicare i dati degli assistiti alla ASL per motivi di controllo della spesa sanitaria.

Al di fuori di questi casi, esistono altre situazioni in cui il medico può derogare all'obbligo della riservatezza? Sì, in ipotesi particolari in cui si renda necessario tutelare la salute di un terzo o della collettività, oppure di un minore, di un soggetto disabile o comunque di un soggetto in situazione di particolare fragilità.
esempio di queste situazioni particolari? se il medico ha in cura un paziente psichiatrico e vi è il rischio concreto e attuale che costui possa costituire un pericolo per l'incolumità di terzi o della collettività, deve segnalare il caso alle competenti autorità (servizi sociali e/o autorità giudiziaria). Oppure se il medico ha in cura un minore e constata che è oggetto di maltrattamenti o abusi, deve segnalare il caso alle medesime autorità. Si tratta di situazioni molto delicate, nelle quali il medico deve agire con la massima prudenza e attenzione, valutando caso per caso. Ma ricordando **che il diritto alla privacy del paziente può essere superato se sussistono ragioni in cui prevale la necessità di tutelare interessi più rilevanti.**

E come si deve comportare il medico a cui l'autorità giudiziaria chiede di rendere testimonianza o di esibire documenti riguardanti un suo paziente? Il medico può sempre opporre il segreto professionale e rifiutarsi di rendere testimonianza o di esibire documenti. In questi casi spetta al magistrato valutare se la testimonianza del medico è indispensabile per la soluzione della vertenza giudiziaria o meno. In tal caso il magistrato può decidere che il segreto debba cedere alle superiori esigenze di giustizia e quindi ordinare al medico di deporre. In questi casi il medico non può più rifiutarsi e al contempo è liberato dall'obbligo del segreto, proprio perché vi è un ordine del giudice.

Il diritto alla privacy esiste anche per il paziente defunto? Le norme del Regolamento Europeo non si applicano alle persone decedute. Bisogna però ricordare che gli eredi del defunto subentrano in tutti i diritti del deceduto, per cui nei confronti di costoro il medico non può opporre il segreto. Se, per esempio, il paziente aveva una polizza assicurativa sulla vita, una volta deceduto i dati sanitari di costui possono essere comunicati agli eredi e anche alla compagnia di assicurazione, visto che nel contratto assicurativo il paziente aveva autorizzato la compagnia ad accedere a tali atti al momento della sua morte.

Per quanto tempo il medico deve conservare i dati dei pazienti nel proprio studio? **Vale la regola generale secondo cui i dati vanno conservati per il tempo necessario al perseguimento della finalità per cui sono stati raccolti. Tradotto nella prassi medica, significa che il medico deve conservare gli atti fin tanto che dura il rapporto di cura.**

In particolare, i dati relativi a ciascun episodio assistenziale, raccolti nella relativa scheda sanitaria, verranno conservati a tempo indeterminato, perdurando il rapporto contrattuale di cura. Al termine del rapporto contrattuale di cura, lo Studio conserverà i dati per un periodo non superiore al termine prescrizionale di legge per la tutela dei propri diritti legali e di difesa.

Il medico che cessa la propria attività come deve comportarsi?

la cessazione dell'attività corrisponde alla cessazione del rapporto di cura.

La conservazione degli atti per tutti questi anni può non essere agevole… E' vero, però bisogna tener conto che potrebbero (anche solo come ipotesi teorica) insorgere contestazioni, vertenze o cause fra medico e paziente e se il medico non dispone più della documentazione clinica non ha nemmeno strumenti per dimostrare la correttezza del suo operato. Conservare i documenti, quindi, significa anche conservare le prove della propria correttezza professionale.

Il medico, nel proprio studio, deve predisporre "distanze di cortesia" o sistemi di chiamata numerica? A differenza delle strutture sanitarie pubbliche o private, che sono locali aperti al pubblico e dove è obbligatorio adottare misure per la riservatezza dei pazienti, negli studi medici privati, che non sono locali aperti al pubblico, non è obbligatorio adottare simili accorgimenti. Tuttavia il medico (e il personale del suo studio) deve comunque rispettare la riservatezza dei pazienti, per cui vanno evitati tutti i comportamenti che possano essere poco rispettosi della privacy di ognuno. Sta al medico individuare, nel concreto, le modalità più idonee.

A telefono il medico può divulgare dati sanitari dei pazienti? Per esempio comunicare l'esistenza di una certa patologia? Per i colloqui telefonici vale la stessa regola prevista per i colloqui di persona. Quindi al diretto interessato si può comunicare ogni informazione sanitaria, sia di persona che per telefono. Ai soggetti terzi, anche se familiari, la comunicazione (di persona o per telefono) è possibile solo con il consenso del diretto interessato.

Si può usare Whatsapp o strumenti simili nel rapporto medico-paziente? Gli strumenti di chat o messaggistica non danno alcuna garanzia legale sull'identità del mittente. Detto in altre parole, mentre al telefono si ha la ragionevole possibilità di identificare colui che sta dall'altra parte della cornetta perché se ne conosce la voce, nelle chat o nei messaggi non c'è modo per avere una minima sicurezza su chi c'è dall'altra parte. Si tratta di strumenti certamente molto utili nelle relazioni quotidiane, ma non sono il mezzo migliore per comunicare e trasmettere dati sensibili come quelli inerenti la salute.
Nel rapporto medico-paziente puo' capitare lo scambio di dati particolari (sensibili), soprattutto tramite Whatsapp e Facebook Messenger. Tuttavia non è consigliabile affidarsi a tali strumenti, sia per problemi di sicurezza delle informazioni sia per problemi di non aderenza al GDPR e Deontologia medica

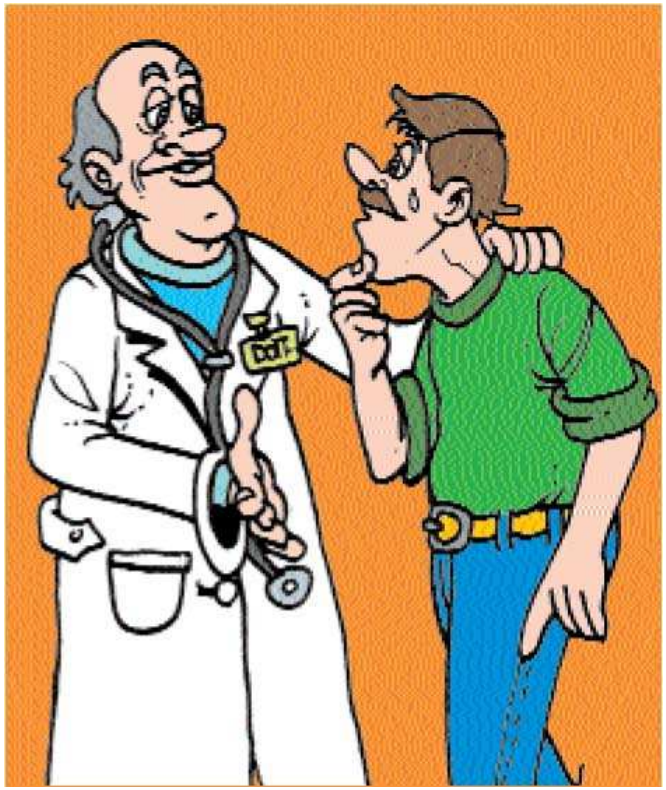
Veniamo ora ai documenti che contengono dati sanitari. Per esempio, i certificati di malattia devono riportare la diagnosi? I certificati di malattia per pazienti che sono lavoratori dipendenti devono essere redatti prioritariamente con la procedura telematica, nella quale è previsto che l'indicazione della diagnosi sia portata a conoscenza solo dell'INPS ma non del datore di lavoro. Ma anche per i certificati cartacei vale la stessa regola, e cioè che la diagnosi non deve essere portata a conoscenza del datore di lavoro. Fanno eccezione solo i lavoratori dipendenti delle Forze Armate, della Polizia di Stato e dei Vigili del Fuoco, perché in questi casi il datore di lavoro deve per legge essere a conoscenza del tipo di patologia sofferta dal militare. Ecco perché nei confronti di questi pazienti è tutt'ora obbligatorio il certificato cartaceo e non quello telematico.

E per i bambini che frequentano la scuola? In caso di malattie infettive o diffusive, il medico è tenuto alla segnalazione, che però deve essere fatta alla ASL e non alla scuola. La scuola, quindi, non può pretendere alcun certificato di malattia dell'alunno, ma semmai solo un certificato per la riammissione a scuola, una volta superata la malattia. È evidente, quindi, che in questi casi il medico non deve mai indicare alcuna diagnosi nel certificato.

E per i pazienti che non sono né lavoratori dipendenti né studenti? Allora si tratta di certificati di malattia che il paziente chiede per suoi motivi privati. In questi casi deve essere lo stesso paziente a chiedere al medico se indicare o meno la diagnosi sul certificato, tenendo conto dell'uso che egli ne vorrà fare.

Oltre ai certificati, ci sono molti altri tipi di documenti che contengono dati sanitari di pazienti…. E’ proprio così. Nella pratica medica i documenti possono assumere moltissime forme: si pensi ai documenti cartacei come le ricette, i certificati, le cartelle cliniche, le perizie, le relazioni e così via. Come sono altrettanti “documenti” anche i cd o le lastre della diagnostica per immagini. Quello che è importante ricordare è che la tutela della legge riguarda i “dati sanitari” indipendentemente del “supporto” che li ospita. Ma siccome il medico è tenuto a tutelare e proteggere la riservatezza dei dati sanitari, è evidente che i supporti che li contengono devono avere un adeguato sistema di protezione.

MODULISTICA



INFORMATIVE E CONSENSI

- MODELLO 1 - INFORMATIVA E CONSENSO TRATTAMENTO DEI DATI PERSONALI RILASCIATO DAL LAVORATORE DIPENDENTE

- MODELLO 2 - INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI (Pazienti)

- MODELLLO 3 - INFOMATIVA DA AFFIGGERE IN STUDIO

MODELLO 1 - INFORMATIVA E CONSENSO TRATTAMENTO DEI DATI PERSONALI RILASCIATO DAL LAVORATORE DIPENDENTE

La scrivente STUDIO _____ comunica che, per l'instaurazione e la gestione del rapporto di lavoro in corso, è titolare di dati Suoi e dei Suoi familiari (1) qualificati come dati personali ai sensi del Regolamento 2016/679.

S'intende per dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile e cioè *interessato,* 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 piu' elementi caratteristici della sua identità fisica, fisiologica, genetica. Psichica, economica, culturale o sociale" (rif. Art. 4 RGDPR)

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1) La informiamo che i dati verranno trattati con il **supporto di mezzi cartacei, informatici o telematici**:
- per l'eventuale **assunzione**, laddove questa non sia già intervenuta;
- per l'elaborazione ed il **pagamento della retribuzione**;
- per l'adempimento degli **obblighi tutti legali** e contrattuali, anche collettivi, connessi **al rapporto di lavoro.**

Alla fine del trattamento i dati verranno accuratamente archiviati applicando le idonee misure minime di sicurezza

BASE GIURIDICA

2) **Il conferimento dei dati è obbligatorio** per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto **l'eventuale rifiuto** a fornirli in tutto o in parte può dar luogo **all'impossibilità per l'azienda di dare esecuzione al contratto** o di svolgere correttamente tutti gli adempimenti, quali quelli di natura retributiva, contributiva, fiscale e assicurativa, connessi al rapporto di lavoro (2). I dati sono raccolti e successivamente trattati per adempiere agli obblighi derivanti dal rapporto di lavoro. Vengono correttamente archiviati adottando le misure minime idonee di sicurezza.

CATEGORIE DI DESTINATARI

3) Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti **i dati raccolti ed elaborati potranno essere comunicati in Italia** e trasferiti all'estero (3) esclusivamente per le **finalità** sopra specificate a:

- Enti pubblici (INPS, INAIL, Direzione provinciale del lavoro, Uffici fiscali);
- Fondi o casse anche private di previdenza e assistenza;
- Studi medici in adempimento degli obblighi in materia di igiene e sicurezza del lavoro;
- Società di assicurazioni;
- Istituti di credito;
- Organizzazioni sindacali cui lei abbia conferito specifico mandato;
- Fondi integrativi (destinare il TFR);
- Organizzazioni imprenditoriali cui aderisce l'azienda;
- Enti Bilaterali previsti dal CCNL
- Centro per l'impiego

NELLA GESTIONE DEI SUOI DATI, INOLTRE, POSSONO VENIRE A CONOSCENZA DEGLI STESSI LE SEGUENTI CATEGORIE DI PERSONE AUTORIZZATE E/O RESPONSABILI INTERNI ED ESTERNI INDIVIDUATI PER ISCRITTO ED AI QUALI SONO STATE FORNITE SPECIFICHE ISTRUZIONI SCRITTE CIRCA IL TRATTAMENTO DEI DATI:

- dipendenti dell'ufficio del personale;
- titolari e dipendenti della società di elaborazione delle paghe, in qualità di incaricati o responsabili esterni *(se nominati)*;
- professionisti o società di servizi per l'amministrazione e gestione aziendale che operino per conto della nostra azienda;

4) In relazione al rapporto di lavoro, LO STUDIO _____ **potrà trattare** dati che la **legge definisce "particolari"** in quanto idonei a rilevare ad esempio:

a) lo stato generale di salute (assenze per malattia, maternità, infortunio o l'avviamento obbligatorio) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche o richieste da Lei stesso/a);
b) (*eventuali altri trattamenti su dati sensibili, sempre strettamente pertinenti all'esecuzione del rapporto di lavoro).*

I dati di natura particolare, concernenti lo stato di salute, che tratta il **medico competente** nell'espletamento dei compiti previsti dal D.Lgs. 81/08 e dalle altre disposizioni in materia di salute e sicurezza sui luoghi di lavoro, per l'effettuazione degli accertamenti medici preventivi e periodici, verranno trattati presso il datore di lavoro esclusivamente dallo stesso medico quale **responsabile** del trattamento, per il quale LO STUDIO _____ chiede espresso consenso (4).

4.a) I dati personali non vengono trasferiti a un paese terzo
4.b) Non è presente profilazione e processo decisionale automatizzato
4.c) il conferimento dei dati è facoltativo a ha diritto di opporsi , in tutto o in parte per motivi legittimi al trattamento dei dati personali pertinenti allo scopo della raccolta. In questo caso non si potrà procedere con l'assunzione.

DIRITTI DELL'INTERESSATO
Relativamente ai dati medesimi si potranno esercitare i diritti previsti dagli artt. 15 - "Diritto di accesso dell'interessato", 16 - "Diritto di rettifica", 17 - "Diritto alla cancellazione", 18 – "Diritto di limitazione al trattamento", 20 – "Diritto alla portabilità dei dati" , 21 - del Regolamento UE 2016/679 nei limiti ed alle condizioni previste dall'art. 12 del Regolamento stesso.
Art. 22 - Diritto di non essere sottoposto a processo decisionale automatizzato, compresa la profilazione

Si ha il diritto di proporre **RECLAMO** all'autorità di controllo GARANTE per la protezione dei dati personali
Mail: www.garanteprivacy.it Piazza di Monte Citorio n. 121 00186 ROMA Centralino telefonico: (+39) 06.696771
Fax: (+39) 06.69677.3785 Per informazioni di carattere generale è possibile inviare una e-mail a: garante@gpdp.it
Posta certificata:

PERIODO DI CONSERVAZIONE

5) Tutti i dati predetti e gli altri costituenti il Suo stato di servizio verranno conservati anche dopo la cessazione del rapporto di lavoro per l'espletamento di tutti gli eventuali adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro stesso (5).

6) La conservazione dei documenti varia da 10 anni a illimitatamente secondo le indicazioni del Prontuario di Selezione per gli Archivi delle Aziende Sanitarie Locali e delle Aziende Ospedaliere redatto dalla Direzione Generale per gli Archivi (Rif. Art 32 RGPD)

7) Titolare del trattamento dei Suoi dati personali è il …….....

8) Responsabile/i del trattamento dei suoi dati è/sono ..... (da riportare qualora in Studio sono stati nominati uno o più responsabili -interni od esterni- del trattamento dei dati personali relativi ai dipendenti).

9) La scrivente non ha nominato la figura del DPO (Data Protection Officer) in quanto non vengono effettuate su larga scala categorie particolari di dati personali come quelli sensibili.

DATI IDENTIFICATIVI DEL DIPENDENTE

Nome _____ Cognome _____ nato il _____a _____ residente a _____ Via _____ in calce identificato/i dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 presta ed esprime il **consenso** (art. 7 RGPD) al trattamento dei propri dati personali per una o piu' specifiche finalità come sopra riportato ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.

Data Firma leggibile

(1)

COGNOME	NOME	REL. DI PARENTELA	FIRMA
.....	.....	.....	.....
.....	.....	.....	.....

Revoca del consenso al trattamento

Si ricorda che, ai sensi dell'art. 7 del Regolamento, è riconosciuta la facoltà di revocare per iscritto il consenso al trattamento dei dati personali.

(1) Da inserire quando si trattano anche dati relativi ai familiari (ad esempio **assegni per il nucleo familiare, permessi per assistenza ai familiari**, ecc.). Il consenso deve essere sottoscritto dai familiari maggiorenni.

(2) Qualora il conferimento di alcuni dati non sia obbligatorio per legge o per contratto è necessario precisare la natura facoltativa, le finalità specifiche, nonché le conseguenze del mancato conferimento.

(3) È' opportuno quindi precisare se il trasferimento dei dati riguarda i paesi UE, o quelli extra UE.

(4) Da inserire nei casi in cui vi siano dipendenti sottoposti a sorveglianza sanitaria ai sensi della normativa vigente.

(5) I dati vanno conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.

INFORMATIVA SUI SISTEMI DI VIDEOSORVEGLIANZA

Lo Studio utilizza un sistema di videosorveglianza degli accessi al solo fine di garantire la sicurezza ed il patrimonio aziendale e prevenire atti illeciti.

Le immagini riprese dalle telecamere sono conservate per un periodo di 24 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa e dell'Autorità Giudiziaria o di Polizia Giudiziaria, dopodiché le immagini si sovrapporranno alle precedenti, cancellandole.

Le immagini sono consultabili solo dal personale incaricato o dall'autorità giudiziaria o di polizia.

Data

Firma per presa visione e accettazione

QUI DI SEGUITO MODELLO ISTANZA DI AUTORIZZAZIONE E ISTRUZIONI …..

MODULO ISTANZA DI AUTORIZZAZIONE
ALL'INSTALLAZIONE DI IMPIANTI AUDIOVISIVI
ai sensi dell'art. 4 della legge 20 maggio 1970 n. 300

All'Ispettorato _____ del Lavoro _____
_____
Via _____
CAP _____ Città _____ Prov ____
Email _____
PEC _____

MARCA DA BOLLO
16,00 EUR

Il/La sottoscritta/o _____ nato a _____ il _____
nella sua qualità di rappresentante legale della Ditta _____
esercente di attività di _____ con sede nel comune di _____
prov _____ CAP _____ via _____ n _____
CCIA di _____ n. _____ P.IVA/CF _____
PEC: _____ tel _____

PREMESSO

1. *(barrare l'opzione che interessa);*
   - ☐ di aver ricevuto visita ispettiva con prescrizione per la violazione dell'art. 4 legge n. 300/70 (verbale n. _____ del _____/_____/20_____);
   - ☐ di non aver ricevuto visita ispettiva con prescrizione per la violazione dell' art. 4 legge n. 300/70;

2. che si rende necessaria l'installazione della apparecchiatura di videosorveglianza per le seguenti motivazioni[1]:
   - ☐ sicurezza del lavoro;
   - ☐ tutela del patrimonio aziendale;
   - ☐ esigenze organizzative e produttive;

   dalle quali può derivare, in via accidentale e/o indiretta e/o potenziale, la possibilità di controllo a distanza dei lavoratori;

3. che sono attualmente in forza all'azienda n. _____ lavoratori;

4. ☐ che non è presente alcuna rappresentanza sindacale in azienda;
   ovvero
   ☐ non è stato raggiunto l'accordo con le rappresentanze sindacali unitarie o aziendali[2]
   (barrare l'opzione che ricorre)

[1] Barrare la/le voce/i interessata/e
[2] Allegare copia

Oppure
per le imprese con più unità produttive ubicate in diverse province della stessa regione ovvero in più regioni:

☐ non è presente alcuna rappresentanza sindacale in tutte le unità produttive;
ovvero
☐ non è stato raggiunto l'accordo con le associazioni sindacali comparativamente più rappresentative sul piano nazionale[3]
(barrare l'opzione che ricorre)

CHIEDE

Il rilascio dell'autorizzazione preventiva per l'installazione delle apparecchiature di videosorveglianza, presso[4]

☐ la sede della ditta
☐ l'Unità Operativa[5] sita in _____, Prov _____, CAP _____
Via _____, così come previsto dall'art. 4 della legge n. 300/1970.

Ovvero:
☐ l'integrazione/modifica ed un impianto di videosorveglianza già autorizzato con provvedimento n. _____ del _____/_____/20_____

A tal fine, consapevole delle responsabilità penali cui si incorre in caso di dichiarazioni mendaci previste dall'art. 76 del D.P.R. 445/2000 e s.m.i. e della decadenza dei benefici eventualmente conseguenti al provvedimento emanato sulla base di una dichiarazione non veritiera

DICHIARA

- che le apparecchiature riprenderanno i luoghi di lavoro connessi alle esigenze per le quali viene richiesta la presente autorizzazione;
- che le telecamere non riprenderanno luoghi riservati esclusivamente ai lavoratori (spogliatoi o servizi);
- ove possibile le telecamere non riprenderanno postazioni di lavoro in maniera continuativa;
- che le immagini non saranno in alcun modo diffuse all'esterno, tranne che per la citata necessità di tempestiva consegna all'Autorità giudiziaria competente qualora si verifichi una fattispecie delittuosa;
- che si provvederà ad informare tutti i lavoratori nelle forme previste dall'art.4, comma 3, della legge n.300/1970;
- che sarà rispettata la disciplina dettata dal d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) e dei successivi provvedimenti del Garante per la Protezione dei Dati Personali;

[3] Allegare copia
[4] Barrare la voce interessata
[5] Se le unità operative sono più di una, allegare l'elenco delle unità operative con il relativo indirizzo per le quali si chiede l'autorizzazione

ALLEGA

1) Relazione, firmata dal Legale Rappresentante, dove illustrare:

   a) le specificazione delle esigenze di carattere organizzativo; produttivo; sicurezza sul lavoro ovvero di tutela del patrimonio aziendale poste a fondamento dell'istanza;

   b) le modalità di funzionamento, di conservazione dei dati e loro gestione nonché i seguenti elementi:

   - ✓ le caratteristiche tecniche delle telecamere interne ed esterne installate;
   - ✓ le modalità di funzionamento del dispositivo di registrazione;
   - ✓ numero di monitor di visualizzazione e loro posizionamento;
   - ✓ fascia oraria di attivazione dell'impianto;
   - ✓ tempi di conservazione delle immagini[1] ed eventuali motivazioni del prolungamento dei tempi oltre le 24/48 ore;
   - ✓ specifiche e modalità di funzionamento del sistema di videosorveglianza.

2) n. 1 marca da bollo da €16,00 per l'istanza e n. 1 marca da bollo da €16,00 per il rilascio del provvedimento (in totale n. 2 marche da bollo da €16,00)[2] da consegnarsi a mano o a mezzo posta[3];

3) n. 1 busta affrancata, se richiesto il recapito del provvedimento autorizzativo a mezzo posta raccomandata a/r[4];

Il sottoscritto dichiara di accettare fin d'ora le eventuali comunicazioni, gli atti e i provvedimenti che verranno inviati al seguente indirizzo di posta elettronica certificata (artt.6 e 48 D.L.vo 82/2005, modificato e integrato con D.L.vo 235/2010): _____

Indicare, di seguito, il nominativo della persona cui potranno chiedersi, se del caso, elementi integrativi e chiarimenti in ordine alla presente istanza cui codesto ufficio potrà inoltrare le comunicazioni:

Sig./Sig.ra _____

email _____

tel. _____ cell. _____

_____, LI _____

_____

Il Legale Rappresentante*

[1] Si fa presente che in linea tendenziale il tempo di conservazione delle immagini è di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa o dell'Autorità Giudiziaria. Per eventuali allungamenti dei tempi di conservazione delle immagini oltre le 24 ore e fino ad un massimo di 7 giorni, qualora ne ricorrano i presupposti di particolare rischiosità o specifiche esigenze tecniche, è necessario fornire una puntuale e specifica motivazione (Cfr. Punto 3.4 del Provvedimento Generale per la Protezione dei Dati Personali in materia di videosorveglianza del 8 aprile 2010 e Parere del Garante per la Protezione dei Dati Personali, prot. n. 176 del 3 settembre 2013, relativo ai chiarimenti sulla durata dell'eventuale conservazione).

[2] In caso di trasmissione dell'istanza in modalità telematica ed acquisizione della trasmissione del provvedimento in modalità analoga, unitamente alla presente istanza, deve essere trasmessa l'apposita "dichiarazione sostitutiva per marca da bollo" presente sul sito.

[3] I tempi per il rilascio del provvedimento autorizzativo decorrono dalla data di consegna a mano o a mezzo posta (in tale caso farà fede il timbro postale) della marca da bollo ovvero dalla data di trasmissione della "dichiarazione sostitutiva per marca da bollo".

[4] Il provvedimento autorizzativo viene in via preferibile trasmesso via PEC. È possibile recapitare il provvedimento a mezzo di posta raccomandata a/r anticipando a questo Ufficio la rispettiva affrancatura oppure è possibile ritirare a mano il provvedimento da parte del Legale Rappresentante o persona debitamente delegata

* Nel caso la presente istanza sia trasmessa per posta certificata a comprova della autenticità della firma dovrà allegarsi fotocopia di un documento di identità del dichiarante in corso di validità.

Il/la sottoscritto/a _____ nella sua qualità di rappresentante legale è *informato/a* che, ai sensi dell'art. 13 d.lgs. n. 196/2003, i dati personali di cui alla presente istanza sono richiesti obbligatoriamente ai fini del procedimento a che gli stessi, trattati anche con strumenti informatici, non saranno diffusi ma potranno essere comunicati soltanto a soggetti pubblici per l'eventuale seguito di competenza e che potrà esercitare i diritti di cui all'art. 7 del d.lgs. n. 196/2003 sulla protezione dei dati.

_____, LI _____

_____

Il Legale Rappresentante

Nota: Ai sensi dell'art.38 del D.P.R. del 28.12.2000, n.445 la dichiarazione è sottoscritta dal legale rappresentante.
Il modulo deve essere obbligatoriamente compilato in modalità digitale cliccando sugli appositi spazi.

ISTRUZIONI

La richiesta di autorizzazione all'Ispettorato Nazionale o Territoriale del lavoro va presentata, dal legale rappresentante della ditta, SOLO se sono presenti lavoratori e in presenza di uno dei seguenti elementi:

1. non sono stati eletti rappresentanti sindacali aziendali (RSA) o rappresentanti sindacali unitari (RSU);
2. pur essendo presenti in ditta RSA o RSU, è stato sottoscritto un verbale di mancato accordo in relazione all'utilizzo dell'impianto di videosorveglianza.

Nella relazione che accompagna l'istanza devono essere esplicitati in maniera dettagliata le motivazioni per le quali si chiede l'autorizzazione all'installazione all'installazione dell'impianto di videosorveglianza (esigenze organizzative e produttive, sicurezza del lavoro, tutela del patrimonio aziendale).

Si riportano qui di seguito alcuni esempi, non esaustivi, di cosa si intenda per ognuna di esse:

- **esigenze organizzative e produttive:**
  - ✓ impiego di macchinari e impianti che necessitano di continuo monitoraggio;
  - ✓ controllo video della qualità di prodotto / processo;
  - ✓ impianti che richiedono frequenti interventi di manutenzione urgente.
- **esigenze di sicurezza sul lavoro:**
  - ✓ necessità di garantire rapido intervento delle squadre di soccorso in caso di infortunio;
  - ✓ svolgimento di attività particolarmente pericolose o impiego di materiali nocivi;
  - ✓ lavoratori che operano in luoghi isolati.
- **tutela del patrimonio aziendale:**
  - ✓ intromissioni o furti denunciati;
  - ✓ presenza di componenti o beni immateriali di elevato valore intrinseco;
  - ✓ presenza di aree aziendali destinate esclusivamente a soggetti qualificati.

Inoltre deve essere descritto in maniera dettagliata la modalità di funzionamento del sistema di videosorveglianza ad es. specificare se l'impianto di videosorveglianza viene tenuto a circuito chiuso, collegato all'intranet aziendale o se è collegato via Internet a postazione remota. È possibile anzi utile allegare le schede tecniche degli elementi che compongono il sistema di videosorveglianza.

Si fa presente che anche la sola installazione e/o la messa in esercizio di impianti audiovisivi e di altri strumenti di controllo prima della prescritta autorizzazione darà luogo all'applicazione delle sanzioni previste dall'art. 38, comma 1, Legge 300/70.

DICHIARAZIONE SOSTITUTIVA PER MARCA DA BOLLO

(art. 47 D.P.R. 28 dicembre 2000, n. 445 – D.M. 10 novembre 2011)

Il /La sottoscritto/a _____

nato a _____ prov. _____ il _____

Codice fiscale _____

nella sua qualità di rappresentante legale della Ditta _____

avvalendosi della facoltà prevista dall'articolo 3 del Decreto Ministeriale 10.11.2011 e consapevole delle sanzioni penali previste dall'articolo 76 del DPR n. 445/2000 e dall'articolo 483 del Codice Penale nel caso di dichiarazioni mendaci, falsità negli atti e uso di atti falsi

DICHIARA

che la marca da bollo n° _____ apposta nello spazio sottostante sull'originale della presente dichiarazione è stata annullata ed è utilizzata **per la presentazione dell'istanza**[1]	che la marca da bollo n° _____ apposta nello spazio sottostante sull'originale della presente dichiarazione è stata annullata e verrà utilizzata **per il rilascio del provvedimento**[2]
Apporre qui la marca da bollo	Apporre qui la marca da bollo

L'originale della presente dichiarazione è custodito dal sottoscritto (con impegno di metterlo a disposizione per eventuali controlli e verifiche ai sensi di legge) presso la sede della Ditta, sita in:

Località _____ - Via _____ n. _____

Luogo e Data _____

Il Dichiarante

_____

[1] L'annullamento del contrassegno, applicato nell'apposito spazio, dovrà avvenire tramite apposizione della data di presentazione della dichiarazione.

[2] La presente dichiarazione, firmata digitalmente, deve essere inviata in modalità telematica.

MODELLO 2 - INFORMATIVA E CONSENSO AL TRATTAMENTO DEI DATI PERSONALI (Pazienti)

I dati personali del paziente sono utilizzati dallo Studio _____che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

Al fine di poter trattare i dati personali dell'utente è necessario ottenere il consenso espresso dello stesso documentato per iscritto avendo precedentemente illustrato oralmente adeguata informativa (Rif. Art 13 paragrafi 1 – 2 RGDPR)

S'intende per dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile e cioè *interessato,* 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 piu' elementi caratteristici della sua identità fisica, fisiologica, genetica. Psichica, economica, culturale o sociale" (rif. Art. 4 RGDPR)

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1) La informiamo che i dati verranno trattati con il supporto dei seguenti **mezzi:**

a) Cartacei
b) Informatici (software gestionali, contabili, ecc.)
c) Telematici (e-mail, sms, social network)
d) Contatti Telefonici tramite operatore di studio

Modalità del trattamento dei dati personali – Il trattamento è realizzato attraverso operazioni, effettuate con o senza l'ausilio di strumenti elettronici e consiste nella raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di tali dati. Il trattamento è svolto dal titolare e dagli incaricati espressamente autorizzati dal titolare.

con le seguenti **finalità**:

1.a **erogazione dei servizi richiesti dal Cliente** o disponibili su portali gestiti da (newsletter, materiale informativo, materiale omaggio) nonché conclusione del contratto di cui è parte l'interessato
1.b Il trattamento è finalizzato unicamente al corretto svolgimento delle attività necessarie per la prevenzione, la diagnosi, la cura, la consulenza (**prestazioni odontoiatriche**), o per le altre prestazioni quali fornire chiarimenti se necessario prescrizioni farmaceutiche e specialistiche.
1.c **Comunicare** i suoi dati Personali al suo **medico curante**
1.d fini **amministrativi e contabili** correlati ai contratti di servizio;

Alla fine del trattamento viene effettuata corretta archiviazione adottando idonee misure minime di sicurezza idonei a garantire la sicurezza e la riservatezza dei dati stessi.
L'eventuale rifiuto nel consentire il trattamento dei dati comporta l'impossibilità di usufruire del servizio richiesto dall'utente.

BASE GIURIDICA

2) Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti. **Il conferimento dei dati personali comuni, sensibili, genetici, relativi alla salute è necessario ai fini dello svolgimento delle attività necessarie per la prevenzione, la diagnosi, la cura, la riabilitazione o per le altre prestazioni da voi richieste, farmaceutiche e specialistiche. Il rifiuto dell'interessato di conferire i dati personali comporta l'impossibilità di adempiere all'attività.**

CATEGORIE DI DESTINATARI e TRASFERIMENTO dei Dati Personali

3) Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di interessati:

– Assistente di Studio odontoiatrico - Igienista dentale -Collaboratori odontoiatri o medici di studio – Personale dipendente - Commercialista – Consulente del Lavoro – Laboratorio odontotecnico - Medico curante previo rilascio del suo consenso specifico

SOLO PER GLI INCARICATI NOMINATI DAL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

I dati personali raccolti non saranno oggetto di diffusione. I dati non sono comunicati a terzi, tranne quando sia necessario o previsto dalla legge. Essi possono venire a conoscenza esclusivamente per le finalità del trattamento. I dati sensibili, genetici e quelli relativi alla salute saranno conosciuti solo ed esclusivamente da parte di personale sanitario della struttura. Si potranno fornire informazioni sullo stato di salute a familiari e conoscenti solo su vostra espressa e specifica indicazione.

PERIODO DI CONSERVAZIONE

4) I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento per l'esecuzione delle prestazioni mediche odontoiatriche e dei servizi richiesti

E' fatta salva in ogni caso **l'ulteriore conservazione** prevista dalla normativa applicabile tra cui quella prevista **dall'art. 2946 cc**

I suoi dati personali trattati per la finalità indicati ai punti : 1.a 1.b 1.c 1.d **saranno trattati fino a revoca del suo consenso .**

I dati di chi non acquista o usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con lo Studio, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di promozione commerciale o ricerca di mercato.

I dati relativi alla **salute** è necessaria per uno specifico interesse e quindi illimitata salvo i suoi diritti. Nel caso in cui i dati non vengano utilizzati gli stessi saranno con diligenza conservati nel pieno rispetto di quanto disciplinato **all'art. 32 RGPD** riguardanti le misure di sicurezza.

L’uso corretto dei dati sarà espletato **da parte dei collaboratori** dello Studio nel rispetto del **segreto professionale.** Sono tenuti a queste cautele anche i professionisti (es: lo specialista) e le strutture che possono conoscerli a seguito dell’attività medica espletata dallo scrivente Studio.

DIRITTI DELL’INTERESSATO

5) Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:

- richiedere la conferma dell'esistenza di dati personali che lo riguardano (**diritto di accesso**);
- conoscerne l'origine;
- riceverne comunicazione intelligibile;
- avere informazioni circa la logica, le modalità e le **finalità** del trattamento;
- richiederne **l'aggiornamento, la rettifica, l'integrazione, la cancellazione**, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti, **la portabilità** dei dati
- nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
- di **revocare** il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca
- il **conferimento** dei dati è facoltativo e si puo’ opporre al trattamento dei dati personali che lo riguardano per motivi legittimi in tutto o in parte . a tal riguardo NON si potrà procedere con l’erogazione della prestazione/servizio

– il diritto di presentare un **reclamo** all'Autorità di controllo che è il GARANTE per la Protezione dei dati personali mail: www.garanteprivacy.it.

Le richieste vanno rivolte al Titolare del trattamento.

6) Titolare del trattamento dei Suoi dati personali è lo Studio_____
Con sede in _____ Via _____

7) Lo scrivente Studio **non** ha la **figura DPO** (Responsabile della protezione dei dati) non effettuiamo su larga scala categorie particolari di dati personali come quelli sensibili
8) Non è presente **profilazione** e nessun **processo** decisionale **automatizzato**
9) Una eventuale **violazione** dei dati personali che la riguardano determini un rischio elevato per i suoi diritti e le sue libertà **comporterà da parte dello Studio un'immediata comunicazione**
10) Il trasferire dati ad un **paese terzo** puo' avvenire solamente nei confronti di quei paesi con garanzie adeguate rispetto alla normativa RGPD

Con la firma del presente modulo si esprime e si presta il consenso al trattamento dei propri dati personali per una o piu' specifiche finalità come indicate in calce alla presente informativa. In qualsiasi momento è possibile ***revocare il consenso*** *senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca.*

Nel rispetto di quanto disciplinato dal RGDP il sottoscritto

Nome_____ Cognome _____ manifesto il mio consenso disciplinato dall'art. 7 RGPD al trattamento dei miei dati personali nelle modalità e finalità sopra riportate.
Tale **consenso** viene da me esercitato dopo aver preso visione dei contenuti della presente informativa ex art. 13 del Regolamento 2016/679 nella sua totalità.

Firma paziente ……

IN CASO DI PAZIENTI MINORENNI:
Io sottoscritto/a Signor/a
Nome e Cognome_____ nato a _____ il _____ residente in _____Via _____ n. _____ cap____

nella qualità di : o Genitore - o Tutore

Nome e Cognome_____ nato a _____ il _____ residente in _____Via _____ n. _____ cap____

Letto e Compreso quanto sopra indicato, fermo restando che i dati personali del minore NON potranno mai essere utilizzati in modo da ledere la sua libertà e/o dignità

o Acconsento **o Non Acconsento**

(Contrassegnare la voce che interessa)

( ) Firma leggibile del genitore se il paziente è minore di **14 anni**
( ) Firma leggibile del tutore legale se paziente minore incapace

……..

MODELLLO 3 - INFOMATIVA DA AFFIGGERE IN STUDIO

Informativa trattamento dei dati personali (ex artt. 13 e 14 Reg.to UE)

Gentili Pazienti,
ai fini previsti dal Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, Vi informo che i dati personali da Voi forniti ed acquisiti dallo Studio Medico _____ saranno oggetto di trattamento nel rispetto della normativa prevista dal premesso Regolamento e dei diritti e degli obblighi conseguenti e che:

- **Finalità del trattamento** – Il trattamento è finalizzato **unicamente al corretto svolgimento delle attività** necessarie per la prevenzione, la diagnosi, la cura, la riabilitazione o per le altre prestazioni da voi richieste, farmaceutiche e specialistiche.
- **Modalità del trattamento dei dati personali** – Il trattamento è realizzato attraverso operazioni, effettuate con o senza l'ausilio di strumenti elettronici e consiste nella raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, cancellazione e distruzione di tali dati. **Il trattamento è svolto dal titolare e dagli incaricati espressamente autorizzati dal titolare.**
- **Conferimento dei dati e rifiuto** – Il conferimento dei dati personali comuni, sensibili, genetici, relativi alla salute è necessario ai fini dello svolgimento delle attività necessarie per la prevenzione, la diagnosi, la cura, la riabilitazione o per le altre prestazioni da voi richieste, farmaceutiche e specialistiche. Il rifiuto dell'interessato di conferire i dati personali comporta l'impossibilità di adempiere all'attività.
- **Comunicazione dei dati** – I **dati personali raccolti non saranno oggetto di diffusione.** I dati non sono comunicati a terzi, tranne quando sia necessario o previsto dalla legge. Essi possono venire a conoscenza esclusivamente per le finalità del trattamento. I dati sensibili, genetici e quelli relativi alla salute saranno conosciuti solo ed esclusivamente da parte di personale sanitario della struttura.

Si potranno fornire informazioni sullo stato di salute a familiari e conoscenti solo su vostra espressa e specifica indicazione.

- **Conservazione dei dati** – I dati personali saranno **conservati per il tempo strettamente necessario all'attività** medica e, in ogni caso, non superiore a dieci anni. Anche in caso di uso di computer, sono adottate misure di protezione idonee a garantire la conservazione e l'uso corretto dei dati anche da parte dei collaboratori dello Studio medico, nel rispetto del segreto professionale. Sono tenuti a queste cautele anche i professionisti (il sostituto, il farmacista, lo specialista) e le strutture che possono conoscerli a seguito dell'attività medica espletata dallo scrivente Studio medico.
- **Titolare del trattamento** – Il titolare del trattamento è il DOTT./ RAGIONE SOCIALE _____ (Codice fiscale: _____), con studio medico/ Poliambulatorio in _____.
- **Diritti dell'interessato** – L'interessato ha diritto:

- di ***chiedere*** al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

- di ***ricevere*** in un formato strutturato, di uso comune e leggibile da dispositivo automatico i **dati personali che lo riguardano** forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti;

- di ***revocare*** il **consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

- - di ***proporre reclamo*** all'Autorità Garante per la Protezione dei dati personali. L'esercizio dei premessi diritti può essere esercitato mediante comunicazione scritta da inviare a mezzo mail: **garante@gpdp.it; PEC : protocollo@pec.gpdp.it o tramite lettera raccomandata a/r all'indirizzo Piazza di Monte Citorio n. 121, IT-00186, Roma**

DOTT. _____

LETTERE DI INCARICO

Modello 4 - Lettera di nomina al RESPONSABILE ESTERNO del trattamento dati
(esempio: COMMERCIALISTA – CONSULENTE DEL LAVORO -)

Modello 5 - Lettera di nomina quale persona autorizzata al trattamento dati

Modello 6 - Lettera di nomina del medico competente per i lavoratori dipendenti sottoposti a sorveglianza sanitaria quale responsabile del trattamento

Modello 7 – Lettera di nomina di Amministratore di Sistema

Modello 4 - Lettera di nomina al RESPONSABILE ESTERNO del trattamento dati

(COMMERCIALISTA – CONSULENTE DEL LAVORO)

Il/La sottoscritto/a Nome Cognome oppure Denominazione in forma Societaria _____, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679,

NOMINA

il Sig./Sig.ra Nome Cognome Responsabile del trattamento dei dati effettuato presso la sede ---------- con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.

In qualità di **Responsabile del trattamento dei dati ha il compito e la responsabilità** di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e **di osservare scrupolosamente quanto** in essa **previsto**, nonchè le seguenti istruzioni impartite dal Titolare.

COMPITI ED ISTRUZIONI PER I RESPONSABILI ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del considerando art. 28 del Regolamento UE 2016/679

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i **dati devono essere TRATTATI**:
  - secondo il **principio di liceità**, vale a dire **conformemente** alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il **principio** fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
  - secondo il **principio** fondamentale della **riservatezza**

- i dati devono essere **raccolti solo per SCOPI**:

– **determinati**, vale a dire che non è consentita la raccolta come attività fine a se stessa;
– **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
– **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
– **compatibili** con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

- i dati devono, inoltre, essere:

esatti, cioè, **precisi e rispondenti al vero** e, se necessario, aggiornati;

– **pertinenti**, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
– **completi**: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
– non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere **raccolti solo i dati** che siano al contempo **strettamente necessari** e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
– **conservati per un periodo non superiore a quello necessario per gli scopi del trattamento** e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati
separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.
Ciascun Responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali.
In ogni caso la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.
In merito alla responsabilità civile, si fa rinvio all'art. 154 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

a) **identificare** e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;

b) **predisporre il registro delle attività di trattamento** da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
il nome e i dati di contatto del Responsabile, del Titolare del trattamento e

- se del caso, i trasferimenti di dati personali verso Paesi terzi;
- descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;

c) definire, per ciascun trattamento di dati personali, **la durata del trattamento e la cancellazione** o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita **l'informativa** ai soggetti interessati. A cura dei Responsabili dovranno inoltre essere affissi i cartelli contenenti l'informativa, in tutti i luoghi ad accesso pubblico, con la precisazione che l'informazione resa attraverso la cartellonistica integra ma non sostituisce l'obbligo di informativa in forma orale o scritta;

e) assicurare che **la comunicazione a terzi e la diffusione dei dati** personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, **solo se prevista** da una norma di legge o regolamento o se comunque **necessaria per lo svolgimento di funzioni istituzionali**. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;

f) adempiere agli **obblighi di sicurezza**, quali:
adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive **misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;**
definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;

h) collaborare con il **Titolare** per l'evasione delle richieste degli interessati e delle istanze del **Garante per la protezione dei dati personali;**

i) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;

j) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(NOME COGNOME)

(firma) _____

Il Titolare del Trattamento
(NOME COGNOME)

(firma) _____

Modello 5 - Lettera di nomina quale persona autorizzata al trattamento dati

Il/La sottoscritto/a Cognome Nome e Denominazione in forma societaria , in qualità del itolare del trattamento dei dati con sede _____, **conferisce** al Sig./Sig.ra Nome incaricato, l'**incarico** nella sua qualità di:

( ) Assistente alla Poltrona
( ) Odontoiatra
( ) Segretaria/Amministrativa di studio/Ambulatorio
( ) Igienista dentale

di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del *titolare del trattamento dei dati*.
A tal fine, vengono fornite **informazioni ed istruzioni** per l'assolvimento del compito assegnato:

- il **trattamento dei dati** deve essere effettuato in modo **lecito corretto e trasparente** ;
- i dati personali devono essere **raccolti** e registrati unicamente per **finalità inerenti l'attività svolta** (**minimizzazione dei dati**);
- è necessaria la **verifica costante** dei dati ed il loro aggiornamento;
- è necessaria la **verifica costante della completezza e pertinenza** dei dati trattati;
- devono essere **rispettate le misure di sicurezza predisposte** dal *titolare/responsabile*;
- in ogni **operazione del trattamento** deve essere **garantita la massima riservatezza** ed in particolare:
  a) **divieto** di **comunicazione e/o diffusione dei dati** senza la preventiva autorizzazione del *titolare/responsabile*;
  b) **l'accesso** ai **dati** dovrà essere **limitato all'espletamento delle proprie mansioni** ed esclusivamente negli orari di lavoro;
  c) la fase di **raccolta del consenso dovrà essere preceduta dalla informativa** ed il consenso al trattamento degli interessati rilasciato in forma scritta;

- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le **proprie credenziali di autenticazione devono essere riservate**;

svolgere le attività previste dai trattamenti secondo le direttive del titolare del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

- **rispettare e far rispettare le norme di sicurezza** per la protezione dei dati personali;
- **informare il responsabile in caso di incidente** di sicurezza che coinvolga dati particolari e non;
- **raccogliere, registrare e conservare i dati presenti negli atti e documenti** contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- **I dati personali interni** allo studio **non possono essere portati all'esterno** del luogo di lavoro
- **eseguire qualsiasi altra operazione di trattamento** nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare del trattamento che provvede anche alla **formazione.**

Inoltre, nel caso in cui Lei sia **abilitato al trattamento dei dati «particolari»** (dati idonei a rivelare **l'origine raziale** ed etnica, le condizioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché **i dati** personali **idonei a rivelare lo stato di salute** e la vita sessuale, ovvero provvedimenti giudiziari), lei **conserverà e custodirà con la massima diligenza i codici sicurezza, parole chiavi** che le consentano l'accesso attraverso **sistemi informatici** o conserverà e custodirà tali dati in **contenitori muniti di serratura** riponendoli nell'archivio di Studio appena terminati le necessità di trattamento.

Le ricordiamo il suo obbligo di **segnalare immediatamente al titolare** del trattamento qualsiasi notizia, di cui lei possa venire in possesso, afferente alla possibile violazione o **perdita di dati personali .**

Gli obblighi relativi alla **riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.**

Si rimanda per tutto quanto non chiaramente specificato nella presente lettera di incarico al rispetto di quanto prescritto dal RGPD.

(*) Per presa visione Persona autorizzata al trattamento dati (NOME COGNOME) _____ (firma)	Il titolare del trattamento (RAGIONE SOCIALE) e/o (NOME COGNOME) _____ (firma)

(*) L'incaricato del trattamento deve restituire controfirmata per «presa visione» e non per «accettazione» in quanto questa lettera s'impegna a dare indicazioni sulle modalità con cui un dipendente o un collaboratore deve svolgere la propria attività attraverso una formula di presa di **buona nota** e attuare le **specifiche istruzioni ricevute.**

Non è altro che un'istruzione operativa che consente al dipendente o collaboratore a svolgere CORRETTAMENTE la propria attività.

ALCUNI ESEMPI dei CONTENUTI DEL PERCORSO FORMATIVO PER INCARICATI AL TRATTAMENTO

1. **LA SICUREZZA DEI DATI PERSONALI: modalità di conservazione in modo sicuro della parola chiave, cambiandole regolarmente ed evitando di condividerle con colleghi , procedura di distruzione di documenti contententi dati personali utilizzando appropriati strumenti di frammentazione, procedure di back-up e procedura di sicura archiviazione dei supporti back-up ecc….**
2. **Procedure che garantiscano un costante aggiornamento dei dati personali custoditi in studio come ad esempio modifiche di indirizzo, Procedure che permettano di spiegare ai clienti nuove o modificate finalità di raccolta dei dati, procedura per la cancellazione dei dati personali, che non siano piu' necessari per le finalità per cui vennero raccolti**
3. **COMUNICAZIONI VIA TELEFONO: procedure che garantiscano una limitazione significativa delle informazioni personali che vengono trasferite via telefono, eventualmente eseguite da conferme scritte.**
4. **RICHIESTA DI ACCESSO DA PARTE DEGLI INTERESSATI: il diritto che hanno gli interessati di ricevere copia dei loro dati personali detenuti dallo Studio, il tempo massimo a disposizione dello studio per rispondere a una richiesta di accesso ai dati**

Art. 8 Dlgs 101/08 lettera G recita: Le Regole di Correttezza da Osservare nella raccolta dei dati e le ISTRUZIONI impartite alle persone AUTORIZZATE al TRATTAMENTO dei dati personali vengono svolte sotto l'Autorità diretta del Titolare

Modello 6 - Lettera di nomina del **MEDICO COMPETENTE** per i lavoratori dipendenti sottoposti a sorveglianza sanitaria quale responsabile del trattamento

Il/La sottoscritto/a Nome Cognome o Denominazione forma societaria _____ in qualità di titolare del trattamento dei dati ai sensi del **GDPR 2016/679**,

NOMINA

il Sig./Sig.ra Cognome Nome _____Responsabile del trattamento delle banche dati di seguito individuate e di quelle che in futuro le verranno affidate nell'ambito dello stesso incarico quale medico competente per lo svolgimento dei compiti previsti dal D.Lgs. 81/08.

Nell'espletamento del suo incarico dovrà attenersi alle disposizioni vigenti disposte dalla legislazione **in materia di igiene e sicurezza nei luoghi di lavoro**, e specificamente:

1) i dati personali per i quali Le viene conferito l'incarico potranno essere trattati con il supporto di **mezzi cartacei, informatici o telematici** (indicare le esatte modalità di trattamento utilizzate) per effettuare, in conformità alle norme di legge, la sorveglianza sanitaria prevista dalla normativa cogente.
2) Ferme restando le comunicazioni agli organi sanitari di controllo competenti eseguite in adempimento di specifici obblighi di legge, i soli **giudizi di idoneità** verranno da Lei **comunicati per iscritto al datore di lavoro ed allo stesso dipendente interessato.**

3) In qualità di medico competente **potrà trattare anche dati che la legge definisce "particolari"** in quanto idonei a rilevare lo stato di salute nell'espletamento dei compiti assegnati dal D.Lgs.vo 81/08 e **specificamente nell'effettuazione** di:

- **accertamenti preventivi sull'idoneità alla mansione specifica**;
- **accertamenti periodici** per controllare lo stato di salute del dipendente ed esprimere il giudizio di idoneità alla mansione specifica;

4) Tutti i dati predetti verranno conservati sotto la esclusiva e diretta responsabilità dello stesso medico competente mediante l'istituzione di una **cartella sanitaria** e di rischio **custodita presso il datore di lavoro**. Lei dovrà coordinarsi con l'azienda per l'individuazione e l'applicazione delle necessarie misure di sicurezza atte a garantire la riservatezza ed integrità dei dati.

5) Il medico competente deve **garantire al dipendente** interessato tutti i **diritti previsti dal Regolamento 2016/679** e i **diritti di informazione previsti dalle norme sull'igiene e la sicurezza nei luoghi di lavoro.**

6) I dati della **cartella sanitaria**, dopo la **risoluzione del rapporto di lavoro**, dovranno essere **consegnati in copia al dipendente,** e, nei casi in cui vi è esposizione ad agenti cancerogeni, consegnati in originale all'ente competente.

Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico Il Medico competente (NOME COGNOME) _____ (firma)	Il titolare del trattamento RAGIONE SOCIALE e/o (NOME COGNOME) _____ (firma)

MODELLO 7 – **LETTERA DI NOMINA DI AMMINISTRATORE DI SISTEMA**

Il/La sottoscritto/a Nome Cognome del rappresentante legale, in qualità di rappresentante legale della Ragione sociale, titolare del trattamento dei dati ai sensi del Regolamento UE 2016/679, affida al Sig./Sig.ra Nome Cognome dell'amministratore l'incarico di amministratore di sistema addetto alla gestione, responsabile del trattamento dei dati personali.

Definizione delle funzioni
Per sua interpretazione "scolastica" l'amministratore di sistema o, ***tecnico sistemista di rete*** *che a dir si voglia,* ***è una figura professionale che approfondisce le competenze di un tecnico hardware e software*** *soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, i livelli di sistemistica e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione.*

Si occupa quindi essenzialmente di ogni tipo di rete informatica, comprese quelle a cui non si accede via web, *come le reti intranet e, non per ultimo implementa i sistemi di sicurezza del networking nonché definisce le procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte gli utenti,* ***cura****ndo* ***interventi di conservazione dei dati attraverso debite soluzioni di "backup"*** *e progettando le attività di supporto al "*disaster recovery*".*
Quindi, come si può dimostrare speditamente, l'amministratore di sistema durante l'espletamento dei suoi incarichi, pur se meramente tecnici, ha un considerevole impatto di responsabilità sui dati aziendali*.*

(v. slide 87)

Caratteristiche
Indubbiamente riveste sul piano operativo una certa professionalità all'interno dell'azienda ma, in realtà, nella nuova rielaborazione europea non appare un chiaro riferimento a tale figura pur se implicitamente richiamata per le sue specifiche competenze tecniche la dove, in capo al titolare del trattamento e/o all' eventuale responsabile nominato, spetta il compito di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento UE 27 aprile 2016 n.679).

Non si parla in questo ambito di quali siano le “misure adeguate” ma sicuramente sono superiori a quelle misure minime di sicurezza cui eravamo abituati con l’allegato B del codice del 2003 e cioè credenziali di autorizzazione, aggiornamenti software e via discorrendo.
Il tecnicismo poi ricordato nelle procedure descritte nello stesso articolo – quali la cifratura dei dati, il loro ripristino in caso di incidenti e le verifiche periodiche delle misure tecniche adottate – lasciano intravvedere una necessaria partecipazione di personale specialistico esperto nella gestione e nella trattazione informatica dei dati personali, così come la necessità di un suo intervento tecnico sin dalle fasi di progettazione e protezione dei dati – la cosiddetta privacy by design e privacy by default – di cui all’art. 25 del medesimo Regolamento UE.
Volendo andare oltre, la prima persona che dovrebbe rendersi conto di un eventuale violazione o perdita dei dati, accidentale od intenzionale che sia, è proprio l’amministratore di sistema che, con la sua attività quotidiana, svolge routine di sicurezza informatica volte a garanzia della struttura informatica.
Siamo in questo caso nell’ambito del cosiddetto “data breach” argomento pregnante nelle attuali discussioni informatico giuridiche e che merita un’alta attenzione, per via delle implicazioni e degli incombenti a carico del titolare del trattamento dei dati.

Sono nelle menti di tutti, ad esempio, i recenti casi Unicredit, Yahoo ed Equifax dove numerosissimi profili (dati personali) sono stati indebitamente acquisiti attraverso attività di hackeraggio a seguito di falle nel sistema informatico aziendale, di fatto mal protetto e mal vigilato.
Il tema della sicurezza informatica non si esaurisce, dunque, solo con semplici installazioni di prodotti antivirus, regole di networking e policy stringenti ma soprattutto con costanti monitoraggi proattivi della rete e delle sue componenti che, ovviamente, devono essere attuati da personale altamente specializzato, ora più che mai viste anche le pesanti sanzioni poste a carico dei titolari del trattamento in caso di inosservanza.
Ne consegue in definitiva un ruolo non di poco conto all'interno di un Sistema Informativo Aziendale dell'amministratore di sistema.

La legislazione

Già previsto agli albori della privacy nella disciplina di protezione dei dati preesistente al Codice del 2003 la dove si definiva l'amministratore di sistema "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione"(art. 1, comma 1, lett. c) d.P.R. 318/1999) viste anche le specificità professionali mirate alla protezione dei dati ed alla sicurezza degli stessi.
Dopo la sua misteriosa scomparsa nel codice del 2003, con provvedimento formale del 27 novembre 2008 ed il successivo del 25 giugno 2009 il Garante della Privacy ha inteso rispecchiare tale figura e specificare meglio le sue attività professionali riportandolo ad un ruolo essenziale nella complessa gestione dei dati e nella doverosa esigenza di elevata protezione degli stessi.

Si è giunti così a definirne l'alta professionalità e responsabilità di vigilanza sui trattamenti informatici all'interno del Sistema Informativo Aziendale pur se sempre relegato alla stretta vigilanza del titolare e/o del responsabile del trattamento.

Considerazioni finali

Stupisce quindi non poco la mancata affermazione, nel nuovo regolamento europeo, di una espressa enunciazione di questa figura essenziale nel processo di trattazione e custodia dei dati considerato che, nella maggior parte delle realtà aziendali, l'amministratore di sistema è personale tecnico qualificato a se stante e non potrà neanche coincidere con analoghe figure di controllo quale il Data Protection Officer che svolge autonome attività di audit nell'ambito della sicurezza informatica.

con i seguenti **COMPITI:**

- **prendere tutti i provvedimenti necessari ad evitare la perdita** o la distruzione **dei dati** e provvedere al ricovero periodico degli stessi **con copie di back-up** secondo i criteri stabiliti dal Titolare/Responsabile del Trattamento dei dati;

- **assicurarsi della qualità delle copie di back-up** dei dati e della loro conservazione in luogo adatto e sicuro;

- **sovrintendere al funzionamento della rete**, comprese le apparecchiature di protezione (**firewall**, filtri);

- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;

- **effettuare interventi di manutenzione hardware e software** su sistemi operativi e applicativi;

- sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;

- fare in modo che sia prevista la disattivazione dei “codici identificati personali” (User-ID), in caso di perdita della qualità che consentiva all’utente o incaricato l’accesso all’elaboratore, oppure nel caso di mancato utilizzo dei “codici identificativi personali” (User-ID) per oltre 6 mesi;

- gestire le password di root o di amministratore di sistema

- collaborare con il responsabile del trattamento dei dati personali;

- collaborare con il custode delle password;

- informare titolare e responsabili sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

L’amministratore di sistema testé incaricato dichiara di essere a conoscenza di quanto stabilito dal Regolamento UE 2016/679 e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme.

Per accettazione dell'incarico L'amministratore del sistema (NOME COGNOME) _____ (firma)	Il titolare del trattamento (NOME COGNOME) _____ (firma)

UTILIZZO APPLICATIVI FORNITI DA AZIENDE TERZE

Modello 12 – UTILIZZO DI APPLICATIVI FORNITI DA AZIENDE ESTERNE

FAC SIMILE LETTERA che il TITOLARE o RESPONSABILE DEL TRATTAMENTO da inviare all'AZIENDA TERZA (SOFTWARE HOUSE) CHE FORNISCE APPLICATIVI/GESTIONALI

……elencare gli applicativi di cui lo STUDIO richiedente si avvale……

LA SCRIVENTE SOFTWARE HOUSE dichiara quanto segue:

gli applicativi in questione sono stati sviluppati e sono costantemente monitorati per verificarne la loro completa corrispondenza alle prescrizioni di cui all'art. 25 del regolamento generale sulla protezione dei dati 679/2016

A tal fine la scrivente software house ha fornito al titolare ed al responsabile del trattamento, che si avvalgono degli applicativi sopraelencati, **appropriate istruzioni** per garantire la piena attuazione operativa dei meccanismi garantistici, introdotti fin dalla progettazione dell'applicativo stesso, e dei meccanismi garantistici, introdotti fin dalla progettazione dell'applicativo stesso, e dei meccanismi di protezione per impostazione predefinita.

ISTRUZIONI OPERATIVE

Modello 8 – Istruzioni Operative Incaricati del Trattamento

Modello 9 – Istruzioni Operative Utilizzo Sistemi Informatici

Modello 10 – Istruzioni Operative Videosorveglianza

Modello 11 – Istruzioni Operativa data breach

(dalla slide 91 alla slide 112)

MODELLO 8 - ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Azienda (*…INDICARE "DENOMINAZIONE DI STUDIO" …)*, conformemente al Regolamento (Ue) 2016/679 (GDPR). I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Azienda.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 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.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Azienda di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

4, ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

• prima della riconsegna, rimuovere eventuali file ivi elaborati;
• quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

B Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

• tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

• devono essere lunghe almeno otto caratteri;
• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
• non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

• Almeno ogni 3 mesi è obbligatorio cambiare la password;
• Ogni password ricevuta va modificata al primo utilizzo;
• La password venga conservata in un luogo sicuro;
• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

C) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;

• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;

• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;

• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

D) Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza della Associazione e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;

• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;

• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

• l'indirizzo del destinatario sia stato correttamente digitato,

• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;

• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

E) Gestione del salvataggio dei dati

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

F) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

G) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

5. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

C) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
• i supporti devono essere archiviati in ambiente ad accesso controllato;
• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido; • quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

6 ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;

L’accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l’accesso ai dati per il tempo strettamente necessario all’assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E’ necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
o in presenza dell’incaricato, far digitare la password dall’incaricato stesso evitando di venirne a conoscenza;
o in assenza dell’incaricato rivolgersi alla persona individuata dall’incaricato quale proprio fiduciario il quale provvederà all’inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all’amministratore di sistema o provvedere, in collaborazione con l’amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l’accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L’amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l’operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all’incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l’accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E’ assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell’intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679.

8. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

9. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

La Direzione

MODELLO 9 - ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. *(…INDICARE "DENOMINAZIONE STUDIO" …)* ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare 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 dal *Responsabile dei sistemi informatici* della *(…INDICARE "DENOMINAZIONE STUDIO" …)*. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche 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.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito

l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali*.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE
Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali*.
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

UTILIZZO DEI SUPPORTI MAGNETICI
Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per *(…INDICARE "DENOMINAZIONE STUDIO" …)* deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno di *(…INDICARE "DENOMINAZIONE STUDIO" …)* è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.

È tassativamente vietata 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 Direzione e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

La Direzione

MODELLO 10 - ISTRUZIONI OPERATIVE VIDEOSORVEGLIANZA

INDICE

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali, volte a garantire l'incolumità pubblica e la sicurezza urbana.

L'Azienda *(…INDICARE "DENOMINAZIONE STUDIO" …)* ha adottato una procedura interna per il trattamento dei dati personali acquisiti mediante l'uso di sistemi di videosorveglianza, che rispetta i principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 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.

2. PRINCIPI GENERALI

La videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;

2) protezione della proprietà;

3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;

4) acquisizione di prove.

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati. Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.
L'attività di videosorveglianza dev'essere effettuata nel rispetto del principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

3. DIRITTI DEGLI INTERESSATI

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al regolamento, in particolare il diritto di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.
Dev'essere assicurato il "diritto all'oblio", ovvero il diritto di ogni singolo individuo a richiedere la cancellazione dei propri dati personali. Vi è, infatti, l'obbligo di cancellazione da parte del titolare del trattamento se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori" (articolo 17 Regolamento 2016/679).

4. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

Secondo quanto afferma il Garante per la Privacy, un sistema di videosorveglianza è a norma quando rispetta i principi di liceità, necessità, proporzionalità e finalità. Attraverso il sistema di videosorveglianza è consentita:

- la registrazione delle immagini se necessarie ad obblighi di legge o per tutelare un interesse legittimo (liceità);
- le riprese devono limitarsi solamente a ciò che è necessario per raggiungere gli scopi prefissati (necessità);
- l'impianto va impiegato solo in luoghi dove è realmente necessario, limitando le riprese alle sole aree interessate ed escludendo la visuale su quelle circostanti (proporzionalità);
- lo scopo della videosorveglianza deve essere esplicito e legittimo nonché limitato alle finalità di pertinenza dei titolari dei dati (finalità).

Il principio generale in materia stabilisce che chiunque installi un sistema di videosorveglianza deve provvedere a segnalarne la presenza, facendo in modo che qualunque soggetto si avvicini all'area interessata dalle riprese sia avvisato della presenza di telecamere già prima di entrare nel loro raggio di azione.
Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.
Il supporto con l'informativa:

• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata, poi rinvii a un testo completo contenente tutti gli elementi, accessibile anche con strumenti informatici e telematici.
Il Titolare del trattamento ha l'obbligo di effettuare la valutazione dell'impatto sulla protezione dei dati personali (DPIA), nel caso in cui la sorveglianza è sistematica su larga scala di una zona accessibile al pubblico (articolo 35 Regolamento 2016/679).

5. VERIFICA PRELIMINARE
Le riprese effettuate per fini di sicurezza e tutela dell'ordine pubblico, con particolare riferimento alla prevenzione di reati o atti di vandalismo e alla sicurezza sul lavoro, costituiscono un'eccezione, e non necessitano dell'obbligo di segnalazione.
Normalmente, per installare un sistema di videosorveglianza, non è necessario l'assenso da parte del Garante della privacy; fanno però eccezione tutti i casi in cui sussiste il rischio di ledere i diritti e le libertà fondamentali o la dignità degli individui ripresi.
Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.
Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso.
La conservazione delle immagini deve avere una durata prestabilita e non eccedente le 24 ore; in situazioni particolari, nelle quali sussiste un elevato fattore di rischio, la durata massima si estende ad una settimana. Nel caso si necessita di una conservazione dei dati più lunga sarà invece necessaria la verifica preliminare del Garante.
Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

Esclusione della verifica preliminare
Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:
a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;
b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;
c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti.
Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio

del silenzio-assenso.
È regola generale che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.
Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza, deve essere preventivamente notificato a questa Autorità.

6. MISURE DI SICUREZZA
Il titolare del trattamento dei dati ha l'obbligo di prendere le misure di sicurezza minime onde evitare la distruzione, la perdita, l'accesso abusivo alle immagini, nonché il loro utilizzo per scopi incoerenti con le finalità previste.
In particolare, i dati raccolti mediante sistemi di videosorveglianza, devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).
È inevitabile che, in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati, le misure minime di sicurezza possano variare anche significativamente.

È tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:
a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

7. RESPONSABILI E INCARICATI
Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini. Deve trattarsi di un numero delimitato di soggetti, specie quando il

titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).
Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento.

8. DURATA DELLA CONSERVAZIONE DATI

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario.
Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario a raggiungere la finalità perseguita.
Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento deve stabilire un termine per la cancellazione o per la verifica periodica.
Generalmente la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che si ritiene non debba comunque superare la settimana.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.
Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

9. SOGGETTI PUBBLICI

I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati.
Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa che:
• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria. Al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.
Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.
In ogni caso, si ribadisce l'auspicio che, l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti.
Avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e da enti territoriali
Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.
Questa Autorità ha già individuato un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale.
In particolare:
a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;
b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.
Il titolare del trattamento è tenuto a richiedere una verifica preliminare all'Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra

individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

10. SOGGETTI PRIVATI

L'installazione di sistemi di videosorveglianza viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Regolamento GDPR non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l'adozione di cautele a tutela dei terzi. In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all'interno di condomini e loro pertinenze (quali posti auto e *box*).

Benché non trovi applicazione la disciplina del Regolamento GDPR, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l'angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l'accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l'abitazione di altri condomini.

11. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679.

12. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

13. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

La Direzione

MODELLO 11 – ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR.

Per **"Violazione di dati"** si intende 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. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.
Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.
- **Rischio elevato**: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

MODULISTICA per la COMUNICAZIONE di VIOLAZIONI dei DATI

Modello 13 - Violazione di dati personali modello di comunicazione al Garante

Modello 14 – Violazione di dati personali modello di comunicazione al Garante «dossier sanitario»

MODELLO 13 - VIOLAZIONE DI DATI PERSONALI MODELLO DI COMUNICAZIONE AL GARANTE

A seguito del recepimento della direttiva 2009/136/Ce ad opera del decreto legislativo 28 maggio 2012, n. 69, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante e, in alcuni casi, al contraente o ad altre persone interessate, le violazioni dei dati personali (Data breach) che detengono nell'ambito delle proprie strutture.

Titolare che effettua la comunicazione

Denominazione o ragione sociale: ……
Provincia……Comune……
Cap. …… Indirizzo ……
Nome persona fisica addetta alla comunicazione……
Cognome persona fisica addetta alla comunicazione……
Funzione rivestita……
Indirizzo Email/PEC per eventuali comunicazioni……
Recapito telefonico per eventuali comunicazioni……
Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

☐ Nuova comunicazione
☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)
☐ Ritiro precedente comunicazione

Breve descrizione del trattamento di dati personali

Quando si è verificata la violazione di dati personali?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati personali?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono coinvolti nella violazione ?

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?

Quale canale è utilizzato per la comunicazione ai contraenti (o alle persone interessate)?

Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione coinvolge contraenti (o altre figure interessate) che si trovano in altri Paesi UE?

☐ Sì

☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

☐ No

☐ Sì

MODELLO 14 - VIOLAZIONE DI DATI PERSONALI MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 4 giugno 2015** *"Linee guida in materia di dossier sanitario"*, i titolari di trattamento dei dati personali effettuati mediante il *dossier* sanitario sono tenuti a comunicare al Garante all'indirizzo: **databreach.dossier@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle proprie strutture (*cfr. punto 7.1. delle predette Linee guida*).

La comunicazione deve essere effettuata entro **48 ore** dalla conoscenza del fatto, compilando il modulo che segue.

Titolare del trattamento del dossier sanitario

Denominazione o ragione sociale: .....

Provincia.....Comune.....

Cap. ..... Indirizzo .....

Nome persona fisica addetta alla comunicazione.....

Cognome persona fisica addetta alla comunicazione.....

Funzione rivestita.....

Indirizzo PEC e/o EMAIL per eventuali comunicazioni.....

Recapito telefonico per eventuali comunicazioni.....

Eventuali Contatti (altre informazioni) .....

Natura della comunicazione

.....

.....

Breve descrizione della violazione dei dati personali trattati mediante il *dossier* sanitario

Quando si è verificata la violazione dei dati personali trattati mediante il *dossier* sanitario?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____

Modalità di esposizione al rischio?

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ **Cancellazione** (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ **Computer**

☐ Rete

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Documento cartaceo

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____

Quante persone sono state colpite dalla violazione dei dati personali trattati mediante il *dossier* sanitario?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati idonei a rivelare lo stato di salute

☐ **Dati relativi a minori**

☐ Dati sanitari relativi a persone sieropositive, a donne che si sono sottoposte a un'interruzione volontaria di gravidanza, a vittime di atti di violenza sessuale o di pedofilia, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, a donne che hanno deciso di partorire in anonimato, i dati riferiti ai servizi offerti dai consultori familiari

☐ Copie per immagine su supporto informatico di documenti analogici

☐ Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati personali trattati mediante il *dossier* sanitario (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

_____

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione resa agli interessati?

_____

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

_____

I medici sono i professionisti che più di tutti, per tradizione millenaria, hanno nel loro patrimonio etico e deontologico la tutela del segreto professionale e della riservatezza dei dati pazienti che hanno in cura. Questo valore deve essere mantenuto vivo e percorrendo questo “binario” etico e deontologico, il medico troverà sempre il modo per affrontare le varie e disparate situazioni in cui si trova ad operare, fondando il suo agire sulla propria coscienza, sensibilità e accortezza.

FONDAMENTALE un “cambio di rotta”, dal vecchio regime formale al nuovo regime sostanziale. La protezione dei dati personali è cambiata, e tutto gira attorno alla responsabilità del Titolare e al suo “dovere” di dar conto di ogni sua scelta.

NON IMPORTA LA
DIMENSIONE DEL PROBLEMA,
IMPORTA LA VOLONTÀ DI RISOLVERLO