MANUALE OPERATIVO PRIVACY

Azienda/Organizzazione

AZIENDA OSPEDALIERA PUGLIESE CIACCIO CATANZARO

SEDE	**SEDE VIA VINICIO CORTESE 25 CATANZARO**
	Responsabile Protezione Dati Dr.ssa Sarah Yacoubi

Data revisione: 27/05/2020

Pur non essendo obbligatorio, il presente manuale operativo e un aggiornamento annuale al regolamento aziendale in materia di protezione dei dati, esso intende rappresentare una guida per tutti collaboratori dell'Azienda in materia di trattamento dei dati personali di persone fisiche.

DATI AZIENDA

Ragione Sociale	AZIENDA OSPEDALIERA PUGLIESE CIACCIO CATANZARO
Partita IVA	*P.IVA/CF: 01991520790*
Codice fiscale	*P.IVA/CF: 01991520790*
Sede legale	VIA VINICIO CORTESE, 25 – 88100 CATANZARO
Contatti	**EMAIL: DIRGENERALE@AOCZ.IT** **PEC: DIRGENERALE@PECAOCZ.IT** **TEL: 09 1883550**
Sito web	WWW.AOCZ.IT
Attività economica	SANITA'
Codici ATECO	DIRGENERALE@AOCZ.IT
Rappresentante legale	DR. GIUSEPPE ZUCCATELLI
Contatti	DIRGENERALE@AOCZ.IT

SEDI

Denominazione	**Azienda Ospedaliera Pugliese Ciaccio**
Tipo	- SANITA' - AMMINISTRATIVA - Operativa
Indirizzo	VIA VINICIO CORTESE, 25 – 88100 CATANZARO

1. DEFINIZIONI

General Data Protection Regulation (GDPR)
Il Regolamento generale per la protezione dei dati personali n. 2016/679 è la normativa europea in materia di protezione dei dati personali di persone fisiche. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016 ma la sua attuazione è avvenuta a distanza di due anni, a partire dal 25 maggio 2018.
Trattandosi di un regolamento non necessita di recepimento da parte degli Stati dell'Unione per cui è attuato allo stesso modo in tutti gli Stati dell'Unione. Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea.

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale
Qualsiasi informazione concernente una persona fisica identificata o identificabile (art. 4 GDPR), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.

Dati particolari
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni 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.

Profilazione
A livello normativo, l'art. 4 del Gdpr definisce la profilazione come: "qualsiasi forma di **trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il **rendimento professionale**, la **situazione economica**, la **salute**, le **preferenze personali**, gli **interessi**, l'**affidabilità**, il **comportamento**, l'**ubicazione** o gli **spostamenti** di detta persona fisica".

Pubblicità comportamentale
La pubblicità comportamentale è una tecnica basata sul tracciamento (tracking) delle attività online degli utenti, al fine di costruire dei profili degli utenti con lo scopo di offrire loro pubblicità più rilevante per gli utenti stessi, e quindi più efficace.

Titolare
Il Titolare del trattamento (data controller) è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"(art.4. par. 1, n.7 GDPR).

Responsabile del trattamento

Responsabile del trattamento Il responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare (art. 4, par. 1, n. 8 GDPR).

Sub responsabile
Il responsabile del trattamento può nominare responsabili di secondo livello a meno che non sia vietato dalle istruzioni del titolare. È comunque il responsabile principale a rispondere di fronte al titolare del trattamento dell'operato dei sub-responsabili. Al sub-responsabile devono essere fornite le istruzioni e deve operare nel rispetto degli obblighi imposti al responsabile del trattamento.

Persona autorizzata
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato
La persona fisica a cui si riferiscono i dati personali.

Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Misure di sicurezza
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che assicurano un livello di protezione adeguato dei dati personali.

Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione
L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

2. RUOLI, COMPITI E NOMINA DEI SOGGETTI

2.1 Titolare del Trattamento

Il **Titolare del trattamento è** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Responsabili del trattamento dati** che assicurino e garantiscano che vengano adottate le misure di sicurezza. Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile del trattamento dei dati** ne assumerà tutte le responsabilità e funzioni.

2.2 Responsabile del Trattamento dati

2.2.1 *Compiti delle persone autorizzate al trattamento dei dati personali*

Il responsabile del trattamento (data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).
Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
Il titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi. Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili. Il titolare deve sempre poter sindacare le decisioni dei responsabili.
Il responsabile ha obblighi di trasparenza, occorre, infatti contrattualizzare il rapporto tra titolare e responsabile specificando gli obblighi ed i limiti del trattamento dati. Il responsabile riceverà, tramite atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi. Inoltre il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR).
Il responsabile ha, poi, l'obbligo di garantire la sicurezza dei dati adottando tutte le misure di sicurezza adeguate al rischio (art. 32 GDPR), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, garantendo la riservatezza dei dati, vincolando i dipendenti, informando il titolare delle violazioni avvenute ed occupandosi della cancellazione dei dati alla fine del trattamento.

2.2.2 *Nomina del Responsabile del trattamento dei dati personali*

La nomina di ciascun Responsabile del trattamento dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere contro firmata dall'interessato per accettazione

2.3 Persona autorizzata al trattamento dei dati personali

2.3.1 Compiti delle persone autorizzate al trattamento dei dati personali

Gli **Incaricati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Responsabile del trattamento**.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:
A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- 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:
  - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del titolare/responsabile;
  - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  - 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 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 datipersonali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari enon;
- 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;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

2.3.2 Nomina delle persone autorizzate al trattamento dei dati personali

La nomina di ciascuna **Persona autorizzata al trattamento dei dati personali** deve essere effettuata dal **Titolare** o dal **Responsabile del trattamento** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

3. NOMINE

Di seguito, è riportato l'organigramma con le funzioni nominate per la gestione della protezione del trattamento dati personali:

SEDE AZIENDA OSPEDALIERA PUGLIESE CIACCIO CATANZARO

Titolare del trattamento:	**GIUSEPPE ZUCCATELLI**	Data nomina: 13/01/2020
Persone autorizzate E nominati	TUTTI I DIRETTORI DI STRUTTURE SEMPLICI E/O COMPLESSE AMMINISTRATIVE E SANITARIE COME RESPONSABILI TRATTAMENTO E I DIPENDENTI COME AUTORIZZATI AL TRATTAMENTO	
DPO:	**DR.SSA SARAH YACOUBI**	Data nomina: 24/05/2018

4. ATTIVITÀ DI TRATTAMENTO DATI PERSONALI

Il presente capitolo riporta l'elenco delle attività di trattamento dati personali e per ognuno sono indicate le seguenti informazioni:

- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

VALUTAZIONE DEI RISCHI – METODOLOGIA UTILIZZATA
Per ogni attività di trattamento è stata eseguita la valutazione dei possibili scenari di rischio. Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

ELENCO ATTIVITA' DI TRATTAMENTO

Nomina	**Titolare del trattamento**
Soggetto	**GIUSEPPE ZUCCATELLI**
Registro	**Registro AZIENDA OSPEDALIERA PUGLIESE CIACCIO CATANZARO**

- Enti pubblici

TRATTAMENTO:SANITA' PUBBLICA
Scheda creata in data: 25/06/2018
Ultimo aggiornamento avvenuto in data: 27/05/2020

Struttura	Amministrazione Sede legale Sede operativa

Personale coinvolto	
Persone autorizzate	TUTTO IL PERSONALE DELL'AOPC ▪ Conservazione ▪ Consultazione ▪ Elaborazione Dr. GIUSEPPE ZUCCATELLI (Titolare) ▪ Conservazione ▪ Consultazione ▪ Elaborazione
Partners - Responsabili esterni	fornitori societa' esterne
Altro	SARAH YACOUBI (Responsabile Protezione Dati DPO)

Processo di trattamento	
Descrizione	funzioni sanitarie per il perseguimento di dati relative alla salute
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Newsletter Albo fornitori Adempimenti agli obblighi di legge Anagrafica clienti- DIPENDENTI
Tipo di dati personali	Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro, accertamenti sanitarie cartelle cliniche referti online) Codice fiscale ed altri numeri di identificazione personale (carte

	sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Particolari (sensibili) Personali
Categorie di interessati	Enti Soggetti o organismi pubblici Clienti ed utenti Dipendenti
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Diffusione al pubblico Clienti ed utenti INPS-INAIL-STRUTTURE SANITARIE CONVENZIONATI AUTORITA' SANITARIE-REGIONE Associazioni ed enti locali
Informativa	Si
Profilazione	Si
Dati particolari	Si
Consenso minori	si
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto sanitario in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale Pacchetto Office
Archiviazione	Armadietto Stanza con diniego di accesso al pubblico Armadio chiuso a chiave
Strutture informatiche di archiviazione	
Archivio Informatico	Struttura interna
Sede di riferimento	Azienda Ospedaliera Pugliese Ciaccio
Personale con diritti di accesso	Pier Raffaelle Martorelli nella qualità di Amministratore del sistema e responsabile servizio informatico- e società sinapsys per l'archiviazione esterna e la direzione medica di presidio per l'archiviazione interna
Note	
Software utilizzati	- Software - Piattaforma Crediti Formativi
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- E' eseguita la DPIA
- Sono definiti i ruoli e le responsabilità
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione
- Dispositivi antincendio

5. ASSET AZIENDALI

Gli asset sono tutti gli strumenti utilizzati dall'organizzazione per trattare e conservare i dati personali quali:

server, computer, sistemi di rilevazione presenze;
programmi software sia installati su dispositivi aziendali che utilizzati in cloud;

archivi relativi a database, cartelle condivise, ecc.

Di seguito la mappatura di tutti gli strumenti:

Denominazione	**Archivio Informatico**
Tipo Struttura	Interna
Sede	Madonna di Cieli-Presidio de Lellis- Presidio pugliese
Personale con diritti di accesso	Personale afferente all'area programmazione e controllo settore CED
Note	Il personale che in servizio presso il CED sono stati autorizzati al trattamento dei dati dalla loro società o/e azienda ospedaliera Pugliese Ciaccio
Software utilizzati	Mire-infor-infosis……

6. ISTRUZIONI OPERATIVE

6.1 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. L'Azienda Ospedaliera Pugliese Ciaccio ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. 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* dell'Azienda Ospedaliera Pugliese Ciaccio Di Catanzaro. 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.

2. 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 da**l** *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 sanitari 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.*

1. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e sanitari

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 sanitari devono essere custoditi in archivi chiusi a chiave.

2. 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.

3. 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 Azienda Ospedaliera Pugliese Ciaccio Di Catanzaro 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 dell'Azienda ospedaliera Pugliese Ciaccio Di Catanzaro 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.

1. 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).

2. 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 e della normativa nazionale in vigore.

3. 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.

4. 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.

6.2 ISTRUZIONI OPERATIVE VIDEOSORVEGLIANZA

INDICE

PREMESSA

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 Ospedaliera Pugliese Ciaccio 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 e dalla normativa nazionale in vigore.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, 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 e normativa nazionale in vigore).

I tempi di conservazione dei dati sanitari

Con i chiarimenti del 7 marzo 2019 il Garante per la protezione dei dati personali ha dato alcune indicazioni con riferimento ai tempi di conservazione dei dati sanitari.

Ai sensi dell'art. 13 par. 2 lett. a) e 14 par. 2 lett a) del GDPR il Titolare del trattamento, nel rendere l'informativa all'interessato, deve indicare anche il periodo di conservazione dei dati oppure, se ciò non è possibile, quali sono i criteri utilizzati per determinare tale periodo.

Al riguardo, con particolare riferimento alla documentazione sanitaria, vi sono diverse norme nel nostro Ordinamento che prevedono tempi di conservazione differenti in base al tipo di referto.

Si fa riferimento, ad esempio:

1.- alla conservazione delle cartelle cliniche di strutture pubbliche o private convenzionate che, unitamente ai relativi referti, vanno conservate illimitatamente nel tempo, secondo quanto stabilito dalla Circolare del Ministero della Sanità del 19 dicembre 1986 n. 900, in cui si afferma esplicitamente che "le cartelle cliniche, unitamente ai relativi referti,
vanno conservate illimitatamente, poichè rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario";

2.- alla documentazione inerente agli accertamenti effettuati nel corso delle visite per il rilascio del certificato di idoneità all'attività sportiva agonistica che deve essere conservata, a cura del medico che ha effettuato la visita, per almeno cinque anni ai sensi dell'art. 5, D.M. 18/02/1982;

3.- alla documentazione iconografica radiologica, che deve essere conservata per un periodo non inferiore a dieci anni ai sensi dell'art. 4 d.m. 14 febbraio 1997.

Più complessa è l'individuazione del tempo di conservazione dei dati nelle ipotesi in cui essi non siano stabiliti da una specifica disposizione normativa, come ad esempio accade per le cartelle cliniche di strutture private non convenzionate.

In simili ipotesi sarà il Titolare del trattamento a dover stabilire tale periodo in modo che i dati sanitari siano conservati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per cui sono raccolti e trattati, nel rispetto del principio di limitazione della conservazione (art. 5, par. 1, lett. e) del GDPR), indicando tale periodo (o i criteri per determinarlo) tra le informazioni da rendere all'interessato.

Come fare tale valutazione?

Caso per caso ed in via preventiva. Sia perché i tempi di conservazione, come detto, devono comparire nell'informativa privacy che viene resa all'interessato al momento della raccolta, sia perché anche la cancellazione/distruzione dei dati (non solo la loro conservazione) potrebbe comportare conseguenze sanzionatorie rilevantissime

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 video sorvegliata.

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 e normativa nazionale in vigore).

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 tecniche ed organizzative 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.

1. 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.

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 GARANTE, 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.

2. 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).

3. 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.

4. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

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

5. 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.

6. 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.

6.3 ISTRUZIONI OPERATIVE DATA BREACH

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) e la normativa nazionale in vigore, 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 e della normativa nazionale in vigore.

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:

- violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;

- violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- 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 de crittografia, 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.

6.4 ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

Premessa

1. Definizioni
2. Adempimenti
3. Modalità di svolgimento delle operazioni
4. Istruzioni per l'uso degli strumenti informatici
   - ❖ Gestione strumenti elettronici (pc fissi eportatili)
   - ❖ Gestione username e password
   - ❖ Installazione di hardware e software

- Gestione posta elettronica aziendale
- Gestione del salvataggio dei dati
- Gestione dei supporti rimovibili
- Gestione protezione dai virus informatici

5. Istruzioni per l'uso degli strumenti "non elettronici"
   a. Distruzione delle copie cartacee
   b. Misure di sicurezza
   c. Prescrizioni per gli incaricati
6. Addetti alla manutenzione
7. Osservanza delle disposizioni in materia di Privacy.
8. Non osservanza della normativa aziendale.
9. Aggiornamento e revisione

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Azienda Ospedaliera Pugliese Ciaccio di Catanzaro , conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. 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) e la normativa nazionale in vigore, 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) e della normativa nazionale in vigore, 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.

1. 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:

b. 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, direttore distruttura che trattano cartella clinica informatizzata). 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 alla struttura 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 achiave;

• 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.

c. 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, inquanto:

• 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 seguenticriteri:

• 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.

d. 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.

e. 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 dell'azienda 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;

f. 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.

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 sanitari 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)/ sanitari devono essere crittografati.

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.

2. 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 sanitari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o sanitari 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 sanitari , 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 sanitari , di un trita documenti

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) /sanitari 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 sanitari 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 sanitari 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 sanitari come carta da riciclo o da appunti.

3. 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 comunicazionescritta;
- 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

4. 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 e della normativa nazionale in vigore.

5. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente Manuale Operativo nonché del regolamento Aziendale in materia protezione dei dati è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

6. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, il presente Manuale è ad integrazioni al Regolamento aziendale protezione dei dati delibera n°308/2018. Le proposte verranno esaminate dalla Direzione.
Il presente Manuale è soggetto a revisione con frequenza annuale.

ZUCCATELLI GIUSEPPE
17.06.2020 10:14:20 UTC