Buona prassi per la gestione del diritto di accesso ai propri dati personali

Approvato con deliberazione n. ..... del .....

Titolare del Trattamento	Diocesi di Sabina – Poggio Mirteto (RI)
Indirizzo sede legale	Piazza Mario Dottori, 14 – 02047 Poggio Mirteto (RI)
Codice Fiscale	91000810571
PEC	diocesi@diocesisabina.it
Responsabile	S.E. Mons. Ernesto MANDARA
DPO	Giuliano PALOTTO

Edizione	Revisione	Data	Descrizione	il Titolare	il DPO
1	0	04/03/2024	Prima emissione	*approvato*	*verificato*

Documento di nr 5 pagine compresa la presente realizzato su format della

0 PREMESSA

Il diritto di accesso ai dati personali rappresenta un diritto primario, più volte ribadito nel regolamento generale europeo (Reg. UE 2016/679, di seguito GDPR) ed in disposizioni nazionali (rif. ex D.Lgs. 196/2003 e s.m.i. e provvedimenti Autorità Garante, di seguito "codice").
La presente buona prassi è da intendersi quale linea guida per i responsabili del trattamento e per chiunque agisce sotto la sua autorità o sotto quella del titolare del trattamento che ha accesso a dati personali (di seguito "incaricato al trattamento" o semplicemente "incaricato") ad adesione volontaria che fornisce presunzione di conformità.

1 DISPOSIZIONE LEGISLATIVA

Nel rispetto del regolamento generale europeo il titolare del trattamento, il responsabile del trattamento e chiunque agisce sotto la sua autorità o sotto quella del titolare del trattamento che ha accesso a dati personali ha l'obbligo di rispondere tempestivamente e compiutamente ad una richiesta di diritto di accesso, valutando la sua fondatezza e evadendo l'istanza secondo il disposto dell'art. 15 GDPR.
Pertanto, l'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione (rif. art. 22, paragrafi 1 e 4 GDPR) e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Nel caso in cui i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate (rif. art. 46 GDPR) relative al trasferimento.
Il titolare del trattamento deve fornire una copia dei dati personali oggetto di trattamento.
In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto dell'interessato a ottenere una copia non deve ledere i diritti e le libertà altrui.
Il regolamento europeo prevede a ciò alcune eccezioni, come ad esempio la comunicazione di dati afferenti ad indagini della polizia giudiziaria, a fronte però di un obbligo generalizzato di evasione corretta e tempestiva della richiesta di accesso.

2 OBIETTIVI DELLA BUONA PRASSI

Il Titolare del trattamento ha realizzato la presente buona prassi ed ha creato le condizioni per renderla fattivamente obiettiva al fine di evitare:

- ritardi nella risposta,
- gestione inappropriata, dovuta ad assenza di specifici punti di contatto, a quesiti rimasti senza risposta od a risposte incomplete o insoddisfacenti,
- mancanza di fiducia, da parte dell'interessato, sulle risposte ottenute,
- incomprensione, vale a dire insufficiente chiarezza, delle informazioni.

Un interessato ha il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include anche il diritto di accedere ai dati relativi alla salute ovvero agli altri dati a carattere speciale (art. 9 GDPR) e ai dati giudiziari (art. 10 GDPR).
Ogni interessato ha pertanto il diritto di conoscere e ottenere comunicazioni in particolare in relazione:

- alla finalità per cui i dati personali sono trattati,
- ove possibile al periodo in cui i dati personali sono trattati,
- ai destinatari dei dati personali,
- alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento.

Tale diritto non deve ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non devono condurre a un diniego totale a fornire all'interessato tutte le informazioni.
Il titolare del trattamento adotta tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online.
Il titolare del trattamento non conserva dati personali al solo scopo di poter rispondere a potenziali richieste.

3 LINEA GUIDA PER LA SODDISFAZIONE DELL'ESERCIZIO DI ACCESSO AI DATI PERSONALI DELL'INTERESSATO

3.1 Punti di contatto

Le istanze di accesso devono essere prioritariamente presentate per iscritto tramite la mail istituzionale dell'ente indicata sul sito web istituzionale e sull'informativa sul trattamento dei dati (rif. Artt. 13 e 14 GDPR).
Per alcune particolari categorie, come ad esempio interessati poco familiari con l'informatica o di una certa età, il front office ed il collegamento telefonico rappresentano indubbiamente le forme più efficienti ed efficaci di contatto.
Sul sito web istituzionale e sull'informativa sul trattamento dei dati (rif. Artt. 13 e 14 GDPR) è indicato un numero telefonico ed i giorni e le ore nelle quali il contatto è disponibile.
Ogni ufficio munito di front office ha esposto un avviso con indicato gli orari di apertura al pubblico, un recapito telefonico ed almeno un recapito di posta elettronica.
Delle modifiche agli orari di apertura e/o ai recapiti di contatto è data adeguata pubblicità.

3.2 Dialogo costruttivo con il richiedente

I soggetti coinvolti nella soddisfazione dell'istanza di accesso sono adeguatamente istruiti e sensibilizzati sulla qualità delle informazioni da raccogliere e sulla definizione delle modalità di risposta che, salvo motivazione oggettiva, non avviene oralmente, invero per via telefonica, ma per posta elettronica tramite mail istituzionale o con posta convenzionale al fine di mantenere traccia oggettiva dell'evasione del diritto di accesso.

3.3 Identità del richiedente

Il diritto di accesso ai propri dati può essere esercitato solo dallo specifico soggetto interessato. È indispensabile accertare sempre l'identità del richiedente (conoscenza personale oppure tramite acquisizione di un documento di riconoscimento). Parimenti, il richiedente deve indicare l'indirizzo al quale dovrà essere spedito la documentazione, ad evasione del diritto di accesso.
La delega scritta ad un terzo è ammessa per l'esercizio del diritto fatto salvo legge contraria.
Nel caso in cui il richiedente chieda dati di terzi ovvero l'evasione del diritto di accesso comporta anche la trasmissione di dati di terzi attenersi alle procedure in materia di accesso civico.

3.4 Tempestività di risposta

Talvolta l'evasione della richiesta è piuttosto complessa e in questo caso è possibile che non tutte le informazioni richieste siano immediatamente disponibili. Questo fatto deve essere chiaramente illustrato all'interessato, che avanza la richiesta di accesso, dando immediata evasione a quelle porzioni della richiesta, che sono immediatamente disponibili, e prendendo contatto con l'interessato per spiegare le ragioni per le quali ulteriori dati potranno arrivare con un certo ritardo di tempo. Di tutti questi contatti deve essere tenuta una traccia, in modo che si possa dimostrare di aver gestito in maniera tempestiva e quanto più possibile efficace la richiesta dell'interessato.
In ogni caso il tempo di evasione della richiesta è fissato in 30 giorni di calendario dalla richiesta. Entro tale termine, su motivato impedimento oggettivo, è possibile fissare un nuovo termine di evasione entro i 60 giorni di calendario successivi, dandone preveniva comunicazione all'interessato.

3.5 Linguaggio di risposta

Chi elabora la risposta ad una richiesta di accesso deve utilizzare nel testo criteri di semplicità, brevità e comprensibilità, in modo da garantirne la completezza e, soprattutto, la comprensibilità per il destinatario.

3.6 Comportamento nel rapporto con l'interessato

Il titolare del trattamento, il responsabile del trattamento e chiunque agisce sotto la sua autorità o sotto quella del titolare del trattamento che ha il compito di evadere l'istanza di accesso non utilizzano comportamenti che possano insinuare nell'interessato il dubbio di malafede del titolare nella gestione di una richiesta di accesso.
Per tale motivo chiunque si trovi ad operare sull'evasione di istanza di accesso assume un atteggiamento onesto e trasparente nei confronti dell'interessato.

4 Sommario

< CARTA INTESTATA DIOCESI SABINA >

Spett.le Presidente del Circolo ANSPI

Poggio Mirteto, 07/03/2024

Un aspetto della recente riforma dello sport è quello riguardante la tutela dei minori che praticano l'attività sportiva; questo tema è disciplinato sia dal Decreto Legislativo 36/2021 che dal Decreto Legislativo 39/2021.

Le ASD e le SSD hanno l'obbligo di designare un "*responsabile della tutela dei minori*", preposto alla prevenzione ed al contrasto di ogni tipo di abuso e di violenza, nonché alla protezione dell'integrità fisica e morale dei giovani sportivi. Tale figura – pur non avendo requisiti di capacità, competenza, conoscenza e moralità stabiliti per legge – ricopre il delicato ruolo di garanzia per la ASD, gli atleti e le loro famiglie.

Viene anche riconfermato l'obbligo per le ASD e SSD di richiedere ai propri collaboratori e lavoratori il certificato penale del Casellario Giudiziale, come già previsto dal D.lgs. 39/2014.

Le norme evocate richiamano la disciplina della responsabilità di società ed associazioni per gli illeciti amministrativi derivanti da reati commessi dai soggetti apicali o dai loro sottoposti; il D.lgs. 39/2021, già in vigore dal 2022, all'articolo 16 impone alla FSN, DSA, EPS la predisposizione di Linee Guida che le ASD e SSD dovranno osservare per la predisposizione di Modelli Organizzativi e Codici di Condotta a tutela dei minori per la prevenzione di qualsiasi violenza o discriminazione sui minori che svolgono attività sportiva.

Le norme sopra indicate richiamano direttamente o indirettamente il D.lgs. 231/2001 che reca la disciplina della responsabilità delle società ed associazioni per gli illeciti amministrativi derivanti da reati commessi dai soggetti apicali (amministratori, direttori generali, coordinatori, ecc.) o dai loro sottoposti (collaboratori, dipendenti, ecc.). Secondo questa disposizione se uno dei soggetti indicati commette uno dei reati espressamente previsti (tra i quali i reati contro i minori), questi sarà responsabile penalmente (secondo il principio "*la responsabilità penale è personale*"), ma la società o associazione (anche sportiva) sarà corresponsabile dell'illecito amministrativo dipendente da quel reato.

Dal coordinamento delle norme illustrate, dunque, le ASD o SSD devono:

- richiedere il certificato del Casellario giudiziario ai collaboratori/lavoratori che sono a contatto con minori,
- dotarsi di un Responsabile per la tutela dei minori,
- predisporre un Modello Organizzativo idoneo a prevenire quei reati ed un Codice di Condotta,
- nominare di un Organismo di Controllo (previsto dal D.lgs. 231/2001) che vigili sull'osservanza del Modello Organizzativo.

L'inosservanza dell'obbligo di richiedere il certificato del casellario giudiziario è punito con la sanzione amministrativa pecuniaria da euro 10.000,00 a euro 15.000,00, mentre l'inadempimento degli obblighi di predisposizione dei modelli organizzativi e di controllo dell'attività sportiva nonché codici di condotta ad esse conformi, è sanzionato secondo le procedure disciplinari adottate dalle Federazioni sportive nazionali, discipline sportive associate, enti di promozione sportiva e associazioni benemerite a cui le ASD e SSD sono affiliate. Restano inoltre ferme le sanzioni previste dal D.lgs. 231/2001 concernente la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.

Al fine di aiutare gli Oratori e i Circoli ANSPI ad adeguarsi al disposto, la Diocesi Sabina è disponibile ad accompagnare le vostre esigenze verso una convenzione economicamente conveniente.

Il/la sottoscritto/a _____, responsabile della **Diocesi di Sabina – Poggio Mirteto**, in qualità di legale rappresentante del Titolare del Trattamento dei Dati Personali

conferisce a

Nome e Cognome: ....., codice fiscale ..... l'incarico di compiere le operazioni di trattamento dei dati sopra elencate nell'ambito delle funzioni di **AMMINISTRATORE DI SISTEMA** (Rif. Art. 28 Reg. UE 2016/679 – GDPR - e Provvedimento Garante 27/11/2008) che è chiamato a svolgere con l'avvertimento che dovrà operare osservando le direttive qui indicate.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- adottare sistemi di controllo che consentano la registrazione degli accessi (log) effettuati dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, *non inferiore a dodici mesi*;
- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;
- fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- gestire le password di root o di amministratore di sistema;
- collaborare e tempestivamente informare il Titolare e/o il Responsabile del Trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

Inoltre, l'espletamento dei compiti di Amministratore di Sistema comprendono altresì l'incarico a compiere le operazioni di trattamento dei dati nell'ambito delle funzioni che è chiamato a svolgere con l'avvertimento che dovrà operare osservando le direttive ricevute. Premesso che le mansioni assegnate richiedono il trattamento di dati personali ivi compresi dati a carattere speciale (art. 9 GDPR) e dati giudiziari (art. 10 GDPR) l'Amministratore di Sistema deve attenersi scrupolosamente ed esclusivamente alle banche dati e alle operazioni descritte nel presente documento.

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 e il loro aggiornamento;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare e/o il Responsabile del Trattamento.

In ogni operazione di trattamento deve essere garantita la massima riservatezza ed in particolare:

- ✓ divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare del Trattamento;
- ✓ l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro; la fase di raccolta dei dati dovrà essere preceduta dall'informativa e dall'eventuale consenso rilasciato nella forma di legge all'interessato;
- ✓ in caso di interruzione, anche temporanea del lavoro verificare che i dati siano inaccessibili ai non autorizzati;
- ✓ le proprie credenziali di autenticazione devono essere riservate; rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- ✓ informare il Titolare e/o il Responsabile del Trattamento in caso di incidente di sicurezza che coinvolga dati sensibili e/o personali; raccogliere, registrare e conservare i dati sia cartacei che su supporto informatico 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.

Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro. Le prescriviamo di limitare il trattamento dei dati a quanto necessario ed indispensabile all'adempimento delle sue mansioni, osservando inderogabilmente le norme di legge, i regolamenti interni, politiche aziendali, circolari, ordini di servizio e le istruzioni comunque impartite dal Titolare e/o il Responsabile del Trattamento.

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono da lei dovuti in base al contratto in essere.

L'Amministratore di Sistema, così come nominato, dichiara di essere a conoscenza di quanto stabilito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679) e si impegna ad adottare tutte le misure necessarie in relazione ai compiti sopra indicati.

Il Presente incarico ha efficacia dalla data di sottoscrizione fino alla risoluzione del rapporto di lavoro per decorrenza dei termini ovvero per qualsiasi causa oppure fino a modifica o revoca da parte del Titolare del Trattamento.

Data: ..... Il Titolare del Trattamento

.....

In pari data per accettazione dell'incarico: L'Amministratore di Sistema .....

MANSIONARIO AMMINISTRATORE DI SISTEMA

COMPITI:

Il Garante per la protezione dei dati personali ha imposto che sia predisposto un "elenco degli amministratori di sistema e loro caratteristiche". Questo adempimento non si esaurisce nella mera predisposizione di una nuova lettera di incarico o nella modifica di quella già esistente ma richiede all'Amministratore di Sistema una serie di "misure e accorgimenti" e, non ultimi, di "adempimenti in ordine all'esercizio dei doveri di controllo da parte del titolare" sulle attività. Con il provvedimento a carattere generale del 27 novembre 2008 dal titolo "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", pubblicato sulla G.U. n. 300 del 24 dicembre 2008, il Garante per la protezione dei dati personali impone ai titolari di trattamenti di dati personali (anche solo in parte gestiti mediante strumenti elettronici) di predisporre un "*amministratore di sistema*" affidandogli, incombenze e responsabilità:

1. gestire il sistema informatico, nel quale risiedono le banche dati di proprietà del Titolare del Trattamento, in osservanza al disciplinare tecnico allegato al Codice della privacy (D.lgs. 30 giugno 2003 n. 196) e sue successive modifiche ed aggiornamenti, attenendosi anche alle disposizioni del Titolare e/o del Responsabile del Trattamento in tema di sicurezza;
2. predisporre ed aggiornare un sistema di sicurezza informatico idoneo, adeguandolo anche alle eventuali future norme in materia di sicurezza. Più specificatamente, in base al sopra citato vigente disciplinare tecnico, fatte salve le successive integrazioni dello stesso, l'Amministratore di sistema dovrà:
    a. assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli incaricati del trattamento dati;
    b. procedere, più in particolare, alla disattivazione dei Codici identificativi personali in caso di perdita della qualità che consentiva all'utente o incaricato, l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 3 (tre) mesi;
    c. adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal GDPR ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità allo stesso Disciplinare tecnico;
    d. adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
    e. indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;
    f. cooperare nella predisposizione del documento programmatico sulla sicurezza per la parte concernente il sistema informatico ed il trattamento informatico dei dati;
    g. vigilare sugli interventi informatici diretti al sistema informatico della Società e, se esistente, sull'impianto di videosorveglianza, effettuati da vari operatori esterni. In caso di anomalie sarà sua cura segnalarli direttamente al Titolare e/o del Responsabile del Trattamento;
    h. predisporre ed implementare le eventuali ulteriori misure minime di sicurezza imposte dal Disciplinare tecnico per il trattamento informatico dei dati a carattere speciale (art. 9 GDPR) e dati giudiziari (art. 10 GDPR) e la conseguente tutela degli strumenti elettronici;
3. coordinare assieme al Titolare e/o al Responsabile del Trattamento le attività operative degli incaricati del trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico;

4. collaborare con il Titolare e/o con il Responsabile del Trattamento per l'attuazione delle prescrizioni impartite dal Garante;
5. comunicare prontamente al Titolare e/o al Responsabile del Trattamento qualsiasi situazione, di cui sia venuta a conoscenza, che possa compromettere il corretto trattamento informatico dei dati personali;
6. verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi installati nei pc presenti;
7. adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate (settore ICT). Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro.

NORME COMPORTAMENTALI:
Scopo della presente procedura è illustrare le norme comportamentali - tecniche cui l'Amministratore di Sistema deve attenersi nello svolgimento delle operazioni di trattamento di dati personali.
In particolare la procedura descrive le regole di ordinaria diligenza che l'Amministratore di Sistema è tenuto ad osservare nel corso della sua prestazione lavorativa e le misure di sicurezza per gli archivi elettronici - cartacei.

LE ISTRUZIONI OPERATIVE PER GLI INCARICATI:
L'Amministratore di Sistema assicura che gli incaricati al trattamento si impegnino a:
- collaborare con l'Amministratore di Sistema;
- utilizzare i dati solo per gli scopi istituzionali, nello spirito della legge e secondo le istruzioni scritte che hanno ricevuto;
- rispettare il segreto di ufficio e professionale, oltre che i requisiti di riservatezza e sicurezza durante l'uso dei dati personali.

IL TRATTAMENTO DEI DATI PERSONALI:
Con il termine trattamento ci si riferisce ad una qualunque operazione effettuata sui dati svolta con o senza l'ausilio di mezzi automatizzati. Il trattamento comprende l'intera vita del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine. Di conseguenza, parliamo di trattamento sia nel caso in cui vengano utilizzati mezzi elettronici o comunque automatizzati, sia altri mezzi che richiedono l'esclusivo apporto umano.

LE REGOLE DI ORDINARIA DILIGENZA:
Nell'esecuzione dei compiti assegnati, chiunque sia autorizzato ovvero sia nella posizione gerarchica o operativa atta a trattare dati personali deve attenersi ad alcune regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento.
Per queste ragioni, nello svolgimento delle proprie mansioni deve prestare particolare attenzione nel:
- non divulgare a terzi estranei le informazioni di cui viene a conoscenza;
- adoperarsi affinché terzi fraudolentemente non entrino in possesso di dati deliberatamente comunicati;
- non fare copie, per uso personale, dei dati su cui si svolgono operazioni di ufficio;
- attenersi scrupolosamente alle istruzioni scritte impartite dal Titolare e/o Responsabile del Trattamento;
- osservare dei criteri di riservatezza;
- trattare i dati in modo lecito e secondo correttezza;
- trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- comportarsi nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- non rivelare o fare digitare le password dal personale di assistenza tecnica;
- non rivelare le password a chicchessia e con qualsivoglia mezzo di comunicazione;
- segnalare qualsiasi anomalia o stranezza al Titolare e/o Responsabile del trattamento.

Qualora si abbandoni temporaneamente la propria postazione di lavoro si deve provvedere a:

- fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali;
- riporre nei cassetti o negli armadi la documentazione cartacea contenente dati personali;
- se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salva schermo del PC con password.

TRATTAMENTO DELLE IMMAGINI:
Il trattamento delle immagini deve essere effettuato esclusivamente in conformità alle suddette finalità, nel rispetto dei principi fondamentali sanciti dall'art. 5 del Regolamento Generale sulla Protezione dei Dati e con l'osservanza delle modalità prescritte dall'azienda

MISURE DI SICUREZZA:
Ognuno è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dal Titolare del Trattamento, nonché quelle che in futuro verranno comunicate.

ULTERIORI ISTRUZIONI IN CASO DI TRATTAMENTO DI DATI A CARATTERE SPECIALE E/O GIUDIZIARI:
Le password di accesso alle procedure informatiche che trattano dati a carattere speciale e/o giudiziari devono essere sostituite, da parte del singolo incaricato, almeno ogni tre mesi.
L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi deve essere effettuato con la stessa periodicità.