Croce Rossa Italiana

Regolamento sulla protezione dei dati personali

Regolamento sulla protezione dei dati personali adottato in attuazione del Regolamento (UE) 2016/679

TITOLARE DEL TRATTAMENTO
CROCE ROSSA ITALIANA - COMITATO DI PESARO ODV
Via Saffi n. 8 - 61122 Pesaro (PU)
0721410842
pesaro@cri.it

Croce Rossa Italiana

Sommario

CAPO I – DISPOSIZIONI GENERALI

Art. 1 - Definizioni

1. Il presente regolamento si avvale delle seguenti definizioni:

a) ***"Codice"*:** D.Lgs. n. 196/2003, così come modificato dal D.Lgs. 101/2018;

b) ***"GDPR"*:** il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati personali);

c) ***"Regolamento"*:** il presente Regolamento;

d) ***"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, 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.

e) ***"Dato personale comune"*:** qualsiasi informazione riguardante una persona fisica(interessato), identificata o identificabile. 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 di caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

f) ***"Dato personale particolare"*:** il dato personale che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, (già dati sensibili) nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

g) "***Dati giudiziari***": i dati personali idonei a rivelare condanne penali, reati o connesse misure di sicurezza, oltre che i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

h) ***"Titolare del trattamento dei dati personali"*** *o anche "**Titolare**"*: **il Comitato** o l'**Organizzazione** cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali. Al Titolare, anche unitamente ad altro Titolare, spettano le decisioni in ordine alle modalità del trattamento e agli strumenti utilizzati. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa in materia di protezione dei dati personali.

i) ***"Responsabile del trattamento dei dati personali"*** *o anche "**Responsabile**"*: la persona fisica o giuridica, individuata dal Titolare, a cui viene esternalizzata un'attività o un servizio che richiede connesse operazioni di trattamento di dati personali per conto del Titolare. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione europea o degli Stati membri.

j) **"*Autorizzati*"**: chiunque, sia esso definito "designato" o "incaricato", agisce sotto l'autorità del Titolare o del responsabile che abbia accesso e gestisca dati personali per le funzioni che gli competono;

k) **"*Designati*"**: coloro che operano sotto l'autorità del Titolare e sono stati individuati da questi a svolgere specifici compiti e funzioni di primo livello connessi al trattamento di dati personali;

l) **"*Incaricati*"**: coloro che operano sotto l'autorità del Titolare e svolgono compiti di secondo livello in merito al trattamento dei dati personali;

m) **"*Amministratore di sistema*"**: il personale sistemistico e di networking, che ha facoltà di accesso alle informazioni anche senza i vincoli e le protezioni del livello applicativo;

n) **"*Interessato*"**, la persona fisica a cui si riferiscono i dati personali;

o) *"**Pseudonimizzazione**"*: il trattamento di dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

p) *"**Garante**"*: l'autorità pubblica di controllo indipendente di cui agli artt. 2-bis e 153 e ss. Del Codice, istituita dalla legge 31 dicembre 1996, n. 675, per vigilare sulla corretta applicazione della normativa in materia di protezione dei dati personali.

Art. 2 - Quadro normativo di riferimento

1. Il presente Regolamento tiene conto della seguente normativa:

a) Regolamento 2016/679 "GDPR" del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

b) Codice in materia di dati personali (D.Lgs. n. 196/2003 s.m.i.);

c) D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;

d) Linee guida e raccomandazioni del Garante per la Protezione dei Dati Personali;

Art. 3 - Oggetto

1. Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal Titolare nel rispetto di quanto previsto dal GDPR.

2. Il presente Regolamento sostituisce integralmente ogni altro precedente Regolamento interno in materia di protezione dei dati personali.

Art. 4 - Finalità

1. Il Titolare garantisce che il trattamento dei dati personali, a tutela delle persone fisiche, si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'integrità, alla disponibilità delle informazioni personali e dell'identità personale a prescindere dalla loro nazionalità o della loro residenza.

2. Il Titolare, nell'ambito delle sue attribuzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.
3. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi di competenza del Titolare sono gestiti conformemente alle disposizioni del Codice, del GDPR e del presente Regolamento.

CAPO II – PRINCIPI

Art. 5 - Principi e responsabilizzazione

1. Vengono integralmente recepiti con il presente Regolamento i principi del GDPR per effetto dei quali i dati personali sono:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *("liceità, correttezza e trasparenza");*
   b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali *("limitazione della finalità");*
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati sulla base del principio di *"minimizzazione dei dati";*
   d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati sulla base del principio di *"esattezza";*
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di *"limitazione della conservazione";*
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di *"integrità e riservatezza";*
   g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità *("principio di necessità")*.
2. Il Titolare è competente per il rispetto dei principi sopra declinati ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 6 - Liceità del trattamento dei dati personali comuni, particolari e giudiziari

1. Il presente Regolamento intende recepire le disposizioni del GDPR in ordine alla liceità del trattamento dei dati personali comuni e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle condizioni indicate nell'art. 6 del GDPR.

2. Il Titolare adottando le massime cautele nel trattamento di informazioni personali del proprio personale dipendente tratta i dati, anche di natura particolare o giudiziaria, per le finalità di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, nel rispetto degli obblighi di legge.

3. Il trattamento dei dati particolari e giudiziari del dipendente da parte del datore di lavoro deve avvenire nel rispetto dei principi di necessità e indispensabilità al fine di ridurre al minimo l'utilizzo dei dati personali e, quando non si possa prescindere dall'utilizzo dei dati giudiziari e particolari, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

Art. 7 - La base giuridica del consenso

1. Il trattamento dei dati personali comuni e particolari può essere basato sul consenso, in tale caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente Regolamento è vincolante. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocabile con la stessa facilità con cui è stato prestato.

Art. 8 - Informativa

1. Il Titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, avvalendosi anche del personale autorizzato, apposita informativa secondo le modalità previste dagli artt. 13 e 14 del GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

2. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, nel rispetto delle caratteristiche di cui sopra.

3. Per i trattamenti dei dati svolti dal Titolare connessi alla gestione del rapporto di lavoro sono predisposte apposite informative per personale dipendente.

4. Nel fornire l'informativa, il Titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati personali. È prevista la possibilità di fornire informative "brevi" che richiamino informative più estese messe a disposizione nel sito internet o presso la sede.

Art. 9 - Sensibilizzazione e formazione

1. Ai fini della corretta e puntuale applicazione della disciplina relativa al trattamento dei dati personali e in particolare in merito ai principi, alla liceità del trattamento, al consenso, al diritto di informazione il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della protezione dei dati personali.

2. A tale riguardo, il Titolare organizza, nell'ambito dell'attività formativa del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali finalizzati alla conoscenza

delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

3. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione dell'accountability dell'Organizzazione.

CAPO III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 - Trattamento dei dati personali, ricognizione dei trattamenti e audit interni

1. Il Titolare tratta i dati personali per lo svolgimento delle proprie attività e nel rispetto di quanto previsto da disposizioni di legge, statutarie, regolamentari, contrattuali e nei limiti imposti dal Codice, dal GDPR, dalle Linee Guida e dai provvedimenti del Garante.
2. Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del Titolare, solo da parte dei soggetti appositamente autorizzati, in base al relativo ruolo o alle mansioni che per contratto sono ricoperte.
3. Non è consentito il trattamento da parte di persone non autorizzate. Eventuali autorizzazioni esterne saranno appositamente disciplinate.
4. Ai fini del trattamento, il Titolare provvede, in collaborazione con il Responsabile della struttura (v. art. 14), alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del Titolare medesimo, funzionali alla formazione del registro dei trattamenti così come indicato dall'art. 30 GDPR.
5. L'attività di aggiornamento è posta in essere tramite appositi audit interni effettuati altresì con analisi/verifiche a campione. Gli audit interni richiedono la concreta verifica delle modalità con cui è effettuato il trattamento dei dati su singole pratiche o posizioni, comparate con il Registro delle Attività già adottato, la documentazione inerente il trattamento (informative, ecc…) ed il presente Regolamento.

Art. 11 - Registro delle attività di trattamento e delle categorie di trattamento

1. Il Titolare del trattamento redige un registro, anche in formato digitale, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità nel rispetto dell'art. 30 GDPR.
2. Il registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.
3. Qualora il Titolare svolga l'attività di trattamento in qualità di responsabile esterno, adotta il registro delle attività di trattamento svolte per conto di un Titolare.

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 12 - Diritti dell'interessato

1. Il Titolare deve garantire ed agevolare, nel rispetto della normativa vigente, l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea.

2. Il Titolare si impegna a non utilizzare i dati che, a seguito di verifiche, dovessero risultare eccedenti o non pertinenti o non necessari.

3. Per garantire un trattamento di dati corretto e trasparente, l'Interessato ha diritto di chiedere al Titolare:

- Diritto di accesso: accedere ai propri dati e conoscere chi vi ha avuto accesso (art. 15 GDPR);
- Diritto di rettifica: richiedere l'aggiornamento, la rettifica o l'integrazione dei dati (art. 16 GDPR);
- Diritto alla cancellazione e di limitazione: richiedere la cancellazione («diritto all'oblio») e la limitazione del trattamento se trattati in difformità dalla legge, fatti salvi gli obblighi legali di conservazione (artt. 17 e 18 GDPR);
- Diritto alla portabilità: ricevere, nei casi normativamente previsti, in formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un Titolare del trattamento unitamente al diritto di trasmettere (se possibile) tali dati ad un altro Titolare, senza impedimenti da parte del Titolare del trattamento cui li ha forniti, qualora:
  - il trattamento si basi sul consenso ai sensi dell'art. 6 GDPR, o dell'art. 9 GDPR o su un contratto ai sensi dell'art. 6 GDPR;
  - il trattamento sia effettuato con mezzi automatizzati (art.20 GDPR);

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento. • Diritto di opposizione: opporsi, per motivi legittimi, al trattamento dei dati (art. 21 GDPR).

1. Ai sensi dell'art. 77 GDPR, resta impregiudicato per l'Interessato il suo diritto, qualora ne ricorrano le condizioni, di rivolgere reclamo al Garante per la Protezione dei Dati Personali secondo le modalità indicate sul sito www.garanteprivacy.it .
2. Ogni diritto deve essere valutato anche nel rispetto dei limiti indicati dagli artt. 23 GDPR, 2-undecies e 2duodecies Codice Privacy.
3. Il modulo per esercitare i diritti in materia di protezione dei dati è pubblicato sul sito istituzionale, nell'apposita sezione, oppure presso gli uffici.

Art. 13 - Procedura per la gestione dell'esercizio dei diritti da parte degli interessati

1. I diritti di cui agli articoli 15 e sgg. del GDPR sono esercitati attraverso il modulo "richiesta di esercizio dei diritti dell'interessato", da recapitarsi all'indirizzo di posta elettronica ordinaria del Titolare.
2. È comunque assicurata la possibilità di esercizio dei suddetti diritti alle persone fisiche anche attraverso la consegna del modello cartaceo presso la sede del Titolare.
3. Si specifica che il considerando 49 del GDPR richiede che il titolare del trattamento proceda a rispondere all'istante senza giustificato ritardo ed al più tardi entro un mese.
4. Il Titolare, qualora la richiesta di esercizio dei diritti proposta dall'interessato sia espressa in forma specifica ovvero facilmente riconducibile ad un determinato trattamento, acquisisce informazioni circa l'istanza da parte del Responsabile della struttura coinvolto dal trattamento.
5. Laddove l'istanza di accesso non sia specifica ma generica, il Titolare invia una richiesta di informazioni, tramite messaggio di posta elettronica avente ad oggetto "diritti privacy", ai Responsabili delle strutture in merito ad eventuali attività di trattamento svolte nei confronti dell'interessato.

6. In base alle informazioni raccolte, e a seguito di specifico approfondimento, laddove sia necessario, ai fini della risposta all'istanza, il Titolare, invia entro 30 giorni dalla notifica dell'istanza, risposta scritta, all'indirizzo di posta elettronica o in alternativa all'indirizzo di residenza dell'interessato tramite posta ordinaria.
7. Il Titolare assicura che la trasmissione della risposta all'interessato non leda i diritti e le libertà di soggetti terzi.
8. In caso di reiterate ed emulative richieste di accesso, il Titolare potrà limitarsi a rispondere all'interessato che i dati oggetto di trattamento sono quelli già comunicati in relazione alle precedenti istanze e potrà attribuire allo stesso i costi di copia.
9. Laddove invece, per la complessità della richiesta o per il numero di richieste ricevute, il Titolare non sia in grado di rispettare i tempi sopra previsti, con comunicazione motivata fornita entro un mese dalla domanda, potrà essere indicata all'interessato una tempistica superiore ai 30 giorni, fino a un massimo di ulteriori due mesi dalla richiesta.
10. Terminata la procedura di richiesta di esercizio dei diritti, il Titolare conserva la documentazione nelle modalità più adeguate al fine di mantenerne la riservatezza, l'integrità e la disponibilità per un periodo non inferiore a 10 anni trascorso il quale sarà distrutta.

CAPO V – SOGGETTI

Art. 14 - Titolare del trattamento

1. L'Organizzazione rappresentata ai fini previsti dal GDPR dal Presidente, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
2. In conformità all'assetto organizzativo del Titolare, i soggetti individuati, ciascuno per il rispettivo ambito di competenza, quali autorizzati al trattamento sono distinguibili in due categorie:
    a) Soggetti *Designati* al trattamento (Presidente dell'Organizzazione e Responsabili delle strutture che compongono l'Organizzazione)
    b) Soggetti *Incaricati* al trattamento (tutti gli altri dipendenti, nonché i soggetti che fanno parte del'Organizzazione).
3. I soggetti di cui sopra sono responsabili del rispetto dei principi applicabili al trattamento dei dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.
4. Inoltre, gli stessi soggetti sono tenuti a porre in essere, nell'ambito delle attività di loro competenza, misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.
5. Le misure sono definite e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15 e ss. GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Art. 15 - Soggetti Autorizzati al trattamento: I Designati e gli Incaricati

1. Il GDPR non prevede particolari formalità per l'individuazione dei soggetti che trattano i dati all'interno dell'Organizzazione ma richiede (in ossequio al principio dell'accountability) una tracciabilità delle

autorizzazioni al trattamento. In tal senso il GDPR fa riferimento in più punti al "*personale che ha accesso permanente o regolare ai dati personali*" o a "*le persone autorizzate al trattamento dei dati personali*".

2. Il nuovo Codice della Privacy, abbandonando il concetto di "Lettera di Incarico", prevede più semplicemente che sia il Titolare a individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che effettuano operazioni sotto la propria autorità (art. 2-*quaterdecies* Codice Privacy).

3. A tal fine, con il presente Regolamento, si individuano diversi livelli di autorizzazione funzionale coerentemente con l'organigramma dell'Organizzazione e, in linea generale, si prevede che le autorizzazioni a trattare i dati personali ai sensi dell'art. 2-quaterdecies del codice siano connesse anche alle autorizzazioni relative ai profili informatici assegnati ai vari dipendenti.

4. Si specifica che, sotto il profilo del trattamento dei dati personali, i soggetti autorizzati si suddividono in:

   a) **DESIGNATI**

   Con il presente Regolamento si individuano quali designati al trattamento dei dati, in ragione e nei limiti del loro mandato, le seguenti figure:

   - Il Presidente del Titolare; ○ I Responsabili delle strutture che compongono il la struttura del Titolare.

   Queste figure sono i riferimenti del Titolare, il quale, con il presente Regolamento, impartisce a essi le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati e all'eventuale uso di apparecchiature di videosorveglianza.

   Con il presente Regolamento gli stessi sono informati delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice e dal GDPR. **Istruzioni:**

   Il Presidente e i Responsabili delle strutture (che supportano il Presidente nello svolgimento delle attività), in ossequio del GDPR, devono attenersi alle seguenti istruzioni:

   - verificare la legittimità dei trattamenti di dati personali effettuati nel settore di riferimento;
   - presidiare l'aggiornamento dei registri delle attività di trattamento e il monitoraggio dei rischi per il relativo settore di competenza, comunicando probabili eventi potenzialmente dannosi per gli interessati;
   - predisporre le informative relative al trattamento dei dati personali nel rispetto degli artt. 13-14 del GDPR; ○ definire modalità, mezzi di trattamento e rispettive responsabilità in merito all'osservanza degli obblighi previsti in caso di esercizio di funzioni e servizi mediante accordo di contitolarità ai sensi dell'art. 26 del GDPR;
   - individuare i responsabili esterni e i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
   - predisporre ogni adempimento organizzativo necessario per gestire l'esercizio dei diritti previsti dalla normativa;

Ciascun designato nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il Titolare al fine di:

- comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;
- Informare il Titolare, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali,
- collaborare nella notificazione di una violazione dei dati personali al Garante privacy,
- collaborare nella comunicazione di una violazione dei dati personali all'interessato,
- assistere il titolare nella redazione della valutazione d'impatto sulla protezione dei dati o nell'eventuale consultazione preventiva.

Ciascun designato risponde al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.

Ciascun designato dovrà rispettare, inoltre, le istruzioni indicate nel regolamento dell'Organizzazione.

b) **INCARICATI:**

Con il presente Regolamento si stabilisce che il personale dipendente del Titolare, i tirocinanti, i collaboratori continuativi e/o altri soggetti, che operano sotto l'autorità del Titolare sono autorizzati, in relazione ai compiti loro conferiti, al trattamento dei dati personali nel rispetto delle mansioni ricoperte e nei limiti delle finalità connesse al rapporto di lavoro con l'Organizzazione, coerentemente con quanto previsto dalle norme vigenti e dal presente Regolamento.

Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare autorizzato ai sensi dell'art. 2-*quaterdecies* del Codice nonché ai sensi degli artt. 4 n.10 e art. 29 del GDPR.

Tali soggetti vengono formalmente autorizzati:

- tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare per ciascun nominativo i trattamenti che lo stesso è autorizzato ad effettuare;

Nel secondo caso, l'autorizzazione scritta deve contenere altresì le istruzioni impartite agli incaricati del trattamento.

Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quantomeno contenere un espresso richiamo al presente Regolamento e alle policy in materia di sicurezza informatica e protezione dei dati personali.

Gli incaricati collaborano con il Titolare ed il designato segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

Con il presente Regolamento si impartiscono loro le necessarie istruzioni in relazione all'informativa fornita agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza.

Istruzioni:

In particolare, gli incaricati devono assicurare che nel corso del trattamento i dati siano:

- trattati solo nell'ambito delle funzioni ricoperte e dell'attività regolarmente assegnatagli;

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- trattati con la riservatezza, l'integrità e la disponibilità che la segretezza dell'attività richiede;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- 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 le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal designato.

Gli incaricati dovranno, altresì, rispettare le istruzioni indicate nel regolamento dell'Organizzazione.

Art. 16 - Gli incaricati al trattamento non dipendenti del Titolare o per specifiche attività

1. Tutti i soggetti che svolgono un'attività di trattamento dei dati e che non sono dipendenti del Titolare (quali a titolo meramente esemplificativo i soggetti che operano temporaneamente all'interno della struttura organizzativa del Titolare o che svolgono solo specifici e limitati interventi sui dati personali), devono essere autorizzati nominativamente al trattamento tramite apposito atto scritto di nomina.
2. Questi ultimi sono soggetti agli stessi obblighi a cui sono sottoposti tutti gli incaricati dipendenti del Titolare, salvo specifiche istruzioni afferenti al servizio svolto, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
3. Gli incaricati non dipendenti dal Titolare, valutato caso per caso, possono essere destinatari degli interventi di formazione e di aggiornamento.

Art. 17 - Responsabili del trattamento (RDT) e sub responsabili

1. Il responsabile è il soggetto che, in ragione di un rapporto giuridico, svolge attività di trattamento dei dati per conto del Titolare.
2. Il responsabile è designato dal Titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il Titolare può avvalersi per il trattamento di dati anche particolari, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se nominato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica del Titolare.

4. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

5. Il Titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, può designare quali responsabili del trattamento dei dati personali, unicamente i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato (GDPR, art. 28).

6. I Responsabili del trattamento saranno nominati dal titolare del trattamento utilizzando il modello di nomina adottato dall'Organizzazione o con modello analogo che garantisca i medesimi presupposti. L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento sono condizioni necessarie per l'instaurazione del rapporto giuridico fra le parti.

Art. 18 - Amministratore di sistema

1. L' amministratore di sistema sovraintende alla gestione e alla manutenzione delle banche dati e nel suo complesso, al sistema informatico di cui è dotata l'amministrazione.

2. La nomina dell'amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'Amministratore di sistema è individuale e nominativa e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato con cadenza annuale da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

3. Il Titolare applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, alle quali quest'ultimo è tenuto al rispetto

4. L'amministratore di sistema è destinatario degli interventi di formazione e di aggiornamento.

CAPO VI – SICUREZZA DEI DATI PERSONALI

Art. 19 - Misure di sicurezza

1. Il Titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione, perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per i quali sono stati raccolti.

2. In particolare, il Titolare del trattamento mette in atto misure tecniche, organizzative, di gestione, procedurali e documentali adeguate a garantire un livello di sicurezza adeguato al rischio rispetto ai diritti e alle libertà degli interessati. Tali misure debbono comprendere almeno:

a) la pseudonimizzazione e la cifratura dei dati personali trattati;
b) le procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) le modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 20 - Valutazione d'impatto sulla protezione dei dati (DPIA)

1. La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

2. La DPIA è uno strumento importante per la responsabilizzazione del Titolare in quanto consente allo stesso non soltanto di rispettare i requisiti previsti dal GDPR ma anche di dimostrare che sono state adottate misure appropriate per garantire il rispetto dello stesso.

3. La DPIA sulla protezione dei dati personali deve essere realizzata prima di procedere al trattamento dal Titolare quando un tipo di trattamento, consideratane la natura, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Per "rischio" si intende uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità e per "gestione dei rischi" l'insieme delle attività coordinate al fine di indirizzare e controllare l'Organizzazione.

4. Prioritariamente alla DPIA deve:

a) essere effettuata o aggiornata la ricognizione dei trattamenti;
b) essere effettuata la determinazione in ordine alla possibilità che il trattamento possa causare un rischio elevato per i diritti e le libertà degli interessati.

5. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

6. Laddove la DPIA riveli la presenza di rischi residui elevati, il Titolare è tenuto a richiedere la consultazione preventiva dell'Autorità di controllo in relazione al trattamento ai sensi dell'art. 36, paragrafo 1 GDPR.

Art. 21 - Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

1. Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è punito con le sanzioni previste dagli articoli da 166 a 172 del Codice da parte dell'Autorità di controllo nonché con sanzioni di natura disciplinare.

2. Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento con conseguente violazione del presente Regolamento.

3. Il responsabile del trattamento risponde per il danno causato dal trattamento solamente se non abbia adempiuto agli obblighi previsti dal Codice, dal GDPR e dal presente Regolamento e a lui specificamente diretti o qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare.

4. Il Titolare e il responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 22 - Violazione dei dati personali

1. Non appena rilevata una incidente di sicurezza che potrebbe essere qualificato come violazione dei dati personali, il Responsabile della struttura, anche per tramite di chi ne è venuto direttamente a conoscenza, ne dà immediata notizia al Titolare per mezzo di una e-mail avente ad oggetto "possibile violazione dei dati personali".
2. Qualora, a seguito della valutazione sulla violazione, ci sia un rischio per i diritti e le libertà degli interessati, il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
3. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le stesse possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
4. Se a seguito della predetta violazione, risulti che il rischio di provocare un danno all'interessato è elevato, oltre all'Autorità Garante, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo". Non è richiesta la comunicazione agli interessati laddove siano soddisfatte almeno una delle condizioni indicate al paragrafo 3 dell'art. 34.
5. Il Titolare, coadiuvato dal Responsabile della struttura, dovrà in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'Autorità Garante e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati così come indicato dall'art. 33, paragrafo 5 GDPR.
6. La documentazione di cui al punto precedente dovrà essere messa a disposizione dell'Autorità qualora richiesto.
7. Il Titolare, coadiuvato dal Responsabile della struttura, provvederà a tenere e aggiornare un Registro delle violazioni dei dati.
8. Il responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Art. 23 - Attività di accertamento ispettivo o di richieste istruttorie da parte dell'Autorità

1. Laddove dovesse pervenire una richiesta da parte dell'Autorità o ci fosse un'attività ispettiva è necessario che il Titolare, sia pronto a rispondere a ogni istanza nel rispetto del principio dell'accountability che fonda l'intera struttura del GDPR.
2. All'Autorità dovrà essere presentato e illustrato il Regolamento adottato in materia di protezione dei dati personali e tutta la documentazione attestante il rispetto della disciplina sul trattamento dei dati personali.

3. Su richiesta dei soggetti accertatori, ciascun Responsabile delle strutture, dovrà avere a disposizione i documenti che attestino l'attività svolta in materia di protezione dei dati personali prestando la massima collaborazione.
4. Qualora, al momento dell'attività ispettiva, i documenti non siano disponibili, il Titolare potrà chiedere ai soggetti accertatori un termine congruo per produrre la documentazione richiesta.

Art. 24 - Disposizioni finali

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.
2. Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.