

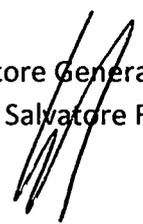
GESTIONE GOVERNATIVA FERROVIA CIRCUMETNEA – CATANIA

ORDINE DI SERVIZIO N. ⁶⁴ /2021 del **20 LUG. 2021**

Per norma e conoscenza di tutto il personale si rende noto il nuovo "Regolamento Aziendale per la protezione dei dati personali Reg. UE 679/2016", che si allega al presente ordine di servizio per farne parte integrante.

D.A. 

Il Direttore Generale
(Dott. ing. Salvatore Fiore)





GESTIONE GOVERNATIVA FERROVIA CIRCUMETNEA

REGOLAMENTO AZIENDALE PER LA PROTEZIONE DEI DATI PERSONALI

Reg.Eu 679/2016

Rev. n. : 01/2021

Data e Luogo,
20 LUG. 2021 CATANIA

Il Titolare al trattamento dei dati



GLOSSARIO

GDPR = Regolamento Generale sulla Protezione dei Dati Personali , Regolamento UE n. 679/2016

RPD = Responsabile della Protezione dei dati (in inglese **DPO** Data Protection Officer)

Data breach = “riuscire a fare breccia”, qualunque violazione dei dati personali

DPIA = Valutazione di impatto sulla protezione dei dati

Privacy by design = Privacy dal momento della sua progettazione. Implica che qualsiasi progetto va realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali

Privacy by default = protezione dei dati per impostazione predefinita, ovvero, misure tecniche e organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento

Audit Privacy è una valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016

GEPD = Garante Europeo della protezione dei dati

Accountability = letteralmente “rendere conto”, ovvero, il Titolare del trattamento si deve responsabilizzare autonomamente nella gestione ed organizzazione della Privacy. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione ha verso chi l'ha scelta e si fonda su: trasparenza intesa come informazioni dell'attività di governo; partecipazione di chiunque al miglioramento delle politiche pubbliche e collaborazione intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo

WP 29 = Working Party Art. 29 (c.d. Gruppo di lavoro art. 29) Organismo consultivo ed indipendente composto da un rappresentante dei Garanti dei dati personali di ogni stato membro, da un rappresentante della Commissione UE e dal Garante europeo della protezione dei dati

INDICE

TITOLO I – PRINCIPI

- Art. 1 - *Finalità*
- Art. 2 - *Principi del trattamento*
- Art. 3 - *Definizioni*

TITOLO II - SOGGETTI DEL TRATTAMENTO DEI DATI

- Art. 4 - *Titolare del trattamento*
- Art. 5 - *Responsabile del trattamento*
- Art. 6 - *Incaricati di trattamento*
- Art. 7 - *Responsabili esterni del trattamento*
- Art. 8 - *Responsabile della protezione dei dati*
- Art. 9 - *Competenze del Responsabile della protezione dei dati*

TITOLO III - TRATTAMENTO DEI DATI PERSONALI

- Art. 10 - *Trattamento dati particolari*
- Art. 11 - *Individuazione di interesse pubblico rilevante*
- Art. 12 - *Trattamento dei dati personali effettuato con sistemi di videosorveglianza*
- Art. 13 - *Registro del trattamento*

TITOLO IV - DIRITTI DELL'INTERESSATO

- Art. 14 - *Diritto di accesso ed alla portabilità dei dati*
- Art. 15 - *Diritto all'oblio*
- Art. 16 - *Diritto alla rettifica dei dati*
- Art. 17 - *Obbligo di informativa*
- Art. 18 - *Informativa sistemi di videosorveglianza*
- Art. 19 - *Consenso*

TITOLO V - MISURE DI SICUREZZA

- Art. 20 - *Misure di sicurezza preventive*
- Art. 21 - *D.P.I.A.*
- Art. 22 - *Procedimento*
- Art. 23 - *Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici*
- Art. 24 - *Misure per dati raccolti con sistemi di videosorveglianza*

TITOLO VI - DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

- Art. 25 - *Definizione di violazione dati personali*
- Art. 26 - *Procedimento in caso di data breach*
- Art. 27 - *Notifica al Garante della privacy*
- Art. 28 - *Comunicazione all'interessato*

TITOLO VII - ENTRATA IN VIGORE

- Art. 29 - *Abrogazioni*
- Art. 30 - *Entrata in vigore del regolamento*

TITOLO I PRINCIPI

Art. 1

Finalità

1. Il presente regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento UE n. 679/2016 (R.G.P.D.) ai fini del trattamento di dati personali per finalità istituzionali in questo Ente.

2. Ai fini del presente regolamento, per funzioni istituzionali si intendono quelle:

- a) previste dalla legge, e dai regolamenti;
- b) in esecuzione di un contratto con i soggetti interessati;
- c) per finalità specifiche e diverse dai punti precedenti purché l'interessato esprima il consenso al trattamento.

3. Il presente regolamento è conforme alle norme e principi costituzionali nonché alle altre disposizioni vigenti sulla materia, incluse le norme non incompatibili del Codice della Privacy, D.Lgs. n. 196/2003.

Art. 2

Principi del trattamento

1. Per le finalità indicate all'art. 1, la Gestione Governativa Ferrovia Circumetnea, effettua il trattamento dei dati personali nel rispetto dei diritti e libertà fondamentali delle persone fisiche nonché del diritto alla riservatezza e all'identità di persone fisiche e giuridiche.

2. In attuazione del comma 1, i dati personali sono:

- trattati in conformità delle norme di legge, cioè in modo lecito e con trasparenza nei confronti dell'interessato;
- corretti, esatti e aggiornati a seguito di intervenute variazioni;
- solo quelli necessari e pertinenti allo scopo specifico, con la riduzione al minimo delle informazioni identificative;
- trattati con adeguate misure di sicurezza in modo da evitare abusi o illeciti o perdita, distruzione o danno accidentale, in conformità del principio di integrità e riservatezza.

Art. 3

Definizioni

Ai fini del presente regolamento si adottano le seguenti definizioni:

- Dati personali: qualunque informazione riguardante una persona fisica identificata o identificabile;
- Trattamento: qualsiasi operazione compiuta con o senza processi automatizzati che prevede la raccolta, la registrazione, l'organizzazione, la strutturazione, conservazione, adattamento o modifica, l'estrazione, consultazione, utilizzo, trasmissione diffusione o altra forma di messa a disposizione di dati personali;
- Profilazione: trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi ad una persona fisica come a titolo esemplificativo, rendimento professionale, situazione economica;
- Archivio: insieme strutturato di dati personali accessibili secondo criteri determinati;
- Pseudonimizzazione: trattamento di dati in modo che non si possa risalire all'identificazione dell'interessato senza informazioni aggiuntive conservate separatamente e soggette a misure di sicurezza;
- Titolare del trattamento: ente locale che anche congiuntamente determina e decide le finalità ed i mezzi del trattamento;
- Responsabile del trattamento: persona fisica o giuridica o ente pubblico che tratta i dati per conto del Titolare del trattamento;

- Responsabile protezione dei dati: persona fisica o giuridica esterna che riveste l'incarico datogli dal Titolare del trattamento;
- Destinatario: persona fisica o giuridica, ente pubblico che riceve comunicazione di dati personali;
- Terzo: chiunque (persona fisica, giuridica, ente pubblico) diverso dall'interessato, dal titolare del trattamento, dal responsabile del trattamento, da ogni incaricato.
- Consenso dell'interessato: ogni manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con cui viene manifestato il suo assenso e viene conferita legittimità al trattamento dei propri dati personali;
- Violazione dei dati personali: ogni diffusione, trasmissione, accesso, comunicazione non autorizzata;
- Dati relativi alla salute: dati personali sensibili sullo stato di salute fisica e mentale di una persona fisica, inclusa la prestazione di servizi di assistenza sanitaria, inclusi i dati genetici e biometrici;
- Dati giudiziari: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

TITOLO II

SOGGETTI DEL TRATTAMENTO DEI DATI

Art. 4

Titolare del trattamento

1. Il Titolare del trattamento dei dati personali è la Gestione Governativa Ferrovia Circumetnea, rappresentata ai fini legali previsti dal Regolamento UE n. 679/2016 dal suo rappresentante legale pro-tempore; lo stesso è responsabile di tutte le decisioni in ordine alle finalità e alle modalità del trattamento dei dati.

2. L'Ente adotta tutte le misure tecniche ed organizzative idonee a garantire che il trattamento è conforme ai principi di cui all'art. 2.

3. Attraverso verifiche periodiche, il Titolare del trattamento, deve vigilare sulla osservanza delle istruzioni impartite ai Responsabili e sul pieno rispetto delle vigenti disposizioni in materia di trattamento dati.

Art. 5

Responsabili del trattamento

1. Il Titolare del trattamento dei dati nomina, con relativa lettera, i Responsabili del trattamento dati della Gestione Governativa Ferrovia Circumetnea.

2. Il Responsabile del trattamento dati dovrà svolgere i compiti specificati, e precisamente:

- garantire che gli incaricati al trattamento siano impegnati alla riservatezza nonché siano in possesso di apposita formazione;
- riferire al Titolare del trattamento ogni violazione di dati personali di cui viene a conoscenza senza ritardo;
- fornire assistenza al Titolare del trattamento per le comunicazioni all'interessato di violazione dei dati personali, sentito se è il caso anche il R.P.D.;
- collaborare alla gestione del registro delle attività di trattamento della struttura/ufficio
- attuare tutto quanto dettagliato nelle lettere di incarico, fornite all'atto di accettazione.

Art. 6***Incaricati del trattamento***

1. Il Responsabile del trattamento è autorizzato a nominare gli incaricati del trattamento, con lettera che:

– individui e delimiti specificatamente l'ambito del trattamento consentito, contiene specifiche istruzioni ed individua le competenze e le attività degli incaricati, tra le quali in particolare:

- la comunicazione agli interessati dell'informativa relativa al trattamento dei dati e alla loro diffusione;
- la collaborazione alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali effettuati dal settore/ufficio di propria competenza;
- effettuare il trattamento dei dati in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per le finalità inerenti l'attività svolta;
- la verifica costante dei dati ed il loro aggiornamento;
- 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:
 - 1) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del *titolare/responsabile*;
 - 2) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
 - 3) 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 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;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

2. La nomina dell'incaricato va comunicata al rappresentante legale dell'Ente il quale deve anche essere informato per ogni variazione o sostituzione degli incaricati del trattamento.

3. Gli incaricati, operano sotto la diretta responsabilità del proprio Responsabile che li ha nominati; in caso di loro inadempimento risponde verso l'Ente, il Responsabile di trattamento di riferimento, ed a seconda della gravità lo stesso incaricato del trattamento.

Art. 7***Responsabili esterni di trattamento***

1. Il Titolare può avvalersi per il trattamento di dati anche sensibili, di soggetti pubblici o privati in qualità di responsabili esterni del trattamento. Gli stessi dovranno nella lettera di accordo e/o contratto specificare le finalità perseguite, la tipologia dei dati, la durata del trattamento, le modalità di trattamento, gli obblighi e i diritti del Responsabile del trattamento.
2. A tali Responsabili esterni si applicano le disposizioni dell'articolo 5 in quanto compatibili.

3. Nel merito delle attività espletate dalla Gestione Governativa Ferrovia Circumetnea per la gestione, convalida, emissione, verifica e tutto quanto in attinenza con la fase di elaborazione e successiva gestione dei titoli di viaggio emessi dalla stessa, ogni rapporto contrattuale dovrà, volta per volta, essere integrato dall'allegato privacy nel quale verranno descritte le fasi operative del trattamento, il soggetto incaricato, la durata del trattamento, la finalità del trattamento il responsabile esterno del trattamento dati e tutto quanto necessario a disciplinare l'uso lecito e corretto dei dati personali forniti a fruitori esterni, o ai quali si abbia accesso.

Art. 8

Responsabile della protezione dei dati

1. Il Titolare del trattamento dei dati nomina con procedura ad evidenza pubblica un soggetto esterno in qualità di Responsabile della protezione dei dati, esperto sulla materia che agisce in posizione di autonomia rispetto al Titolare del trattamento e non ha ulteriori incarichi nell'ente che possano dare adito a conflitti di interesse. Il Responsabile svolge le competenze espressamente attribuite con apposito contratto di servizi.

2. La nomina del RPD va comunicata al Garante privacy ed a tutto il personale in modo che la sua presenza e le sue funzioni del Responsabile siano note a tutti i dipendenti.

3. Il nominativo nonché indirizzo Pec del RPD va pubblicato nel sito dell'Ente nella relativa sezione.

Art. 9

Competenze del Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati va tempestivamente informato di tutte le questioni riguardanti la protezione dei dati personali e, nell'eseguire i propri compiti, considera i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. In particolare:

- informa e fornisce consulenza al Titolare del trattamento o al Responsabile nonché agli altri dipendenti incaricati;
- verifica l'applicazione corretta della disciplina sul trattamento dei dati personali e del GDPR, ferma restando la responsabilità del Titolare e del Responsabile di trattamento; sorveglia le attribuzioni di responsabilità, le attività di formazione e controllo effettuate dal Titolare e del Responsabile del trattamento;
- collabora in sede di audit alla mappatura dei processi e alla individuazione delle non conformità per le quali suggerisce misure correttive. Successivamente sovrintende i monitoraggi periodici delle soluzioni adottate per verificare la necessità di eventuali riesami o sostituzione delle misure;
- funge da tramite con il Garante per la consultazione preventiva, in caso residuino rischi elevati in un trattamento, dopo l'adozione della valutazione di impatto sulla protezione dei dati personali;

TITOLO III

TRATTAMENTO DEI DATI PERSONALI

Art. 10

Trattamento dati particolari

1. Gli uffici della Gestione Governativa Ferrovia Circumetnea trattano eventuali dati particolari, sensibili ai sensi dell'art. 9 GDPR:

- per motivi di interesse pubblico rilevante come specificati nel successivo art. 11;
- se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;

- per diritti dell’interessato in materia di diritto del lavoro e sicurezza sociale e protezione sociale;
- 2. I dati particolari riguardanti lo stato di salute non devono essere divulgati.

Art. 11

Individuazione di interesse pubblico rilevante

Le macroaree che caratterizzano alcuni trattamenti dei dati svolti per interesse pubblico rilevante nell’Ente sono le seguenti:

RAPPORTI DI LAVORO
MATERIA TRIBUTARIA
BENEFICI ECONOMICI ED ABILITAZIONI
ATTIVITA’ DEL PROTOCOLLO
EMISSIONE DEI TITOLI DI VIAGGIO
ACQUISTI E GARE

Art. 12

Trattamento dei dati personali effettuato con sistemi di videosorveglianza

1. Il trattamento dei dati personali effettuato mediante l’uso di sistemi di videosorveglianza richiede apposita informativa agli interessati e questa può essere rilasciata in forma semplificata .

2. Per finalità di tutela della sicurezza urbana, la durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l’uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione in conformità dell’art. 6, co. 9, D.L. n. 11/2009.

Art. 13

Registro del trattamento

1. Il Titolare del trattamento istituisce, in forma scritta tramite un registro le attività di trattamento svolte sotto la propria responsabilità; nel caso particolare la copia dei registri è in possesso sia del singolo Responsabile del trattamento dati che del componente del team privacy interno all’Azienda.

2. Il Registro privacy del Titolare del trattamento deve contenere almeno le seguenti informazioni:

- estremi identificativi e di contatto dell’Ente;
- estremi identificativi e di contatto Responsabile della protezione dei dati;
- finalità del trattamento;
- descrizione delle categorie di interessati;
- descrizione delle categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- eventuali trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale con documentazione delle garanzie in materia di privacy;
- termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

3. In caso di richiesta del Garante, il Registro privacy è messo immediatamente a disposizione.

TITOLO IV DIRITTI DELL'INTERESSATO

Art. 14

Diritto di accesso ed alla portabilità dei dati

1. L'interessato ha sempre diritto di ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano, di averne accesso e di acquisire le seguenti informazioni:

- a) finalità del trattamento;
- b) categoria di dati trattati;
- c) i destinatari a cui i dati personali sono comunicati;
- d) il periodo di conservazione dei dati previsto o se non è possibile, i criteri utilizzati per determinare tale periodo;

2. La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.

Art. 15

Diritto all'oblio

1. L'interessato ha diritto a chiedere previa richiesta scritta, al Titolare del trattamento la cancellazione dei dati personali che lo riguardano:

- se non sono più necessari per le finalità per le quali sono stati raccolti o trattati;

Art. 16

Diritto alla rettifica dei dati

1. L'interessato ha diritto a chiedere previa richiesta scritta, la rettifica da parte dell'Ente, senza ingiustificato ritardo, dei dati personali inesatti che lo riguardano. La rettifica include anche la possibile integrazione dei dati avuto riguardo alla finalità del trattamento.

Art. 17

Obbligo di informativa e contenuto

1. Prima che inizi qualunque trattamento di dati personali il Titolare del trattamento o per tramite dei Responsabili e incaricati del trattamento, fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti, fornite per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.

2. Essa va effettuata:

- in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
- in caso di dati personali non ottenuti presso l'interessato:

3. Non è necessario fornire l'informativa:

- nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
- nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato;
- in presenza di un obbligo di legge

Art. 18

Informativa per utilizzo di sistemi di videosorveglianza

1. Nel caso di utilizzo di sistemi di videosorveglianza per finalità di sicurezza urbana, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata;

2. A tal fine può essere utilizzato un modello di informativa semplificata

Art. 19

Consenso

1. Il consenso al trattamento dei dati non è richiesto all'Ente se agisce per finalità istituzionali.

2. Il consenso può essere richiesto se l'Ente agisce per specifiche finalità diverse da quelle istituzionali ai sensi . In tal caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso secondo le modalità scelte.

TITOLO V

MISURE DI SICUREZZA

Art. 20

Misure di sicurezza preventive

1. L'Ente deve adottare misure che soddisfino la protezione dei dati fin dalla progettazione e della protezione dei dati di default; ovvero, mette in atto misure tecniche ed organizzative adeguate sia prima del trattamento, sia nell'atto del trattamento stesso indicate nel presente titolo.

2. L'Ente in particolare:

- tratta i soli dati necessari per ogni specifica finalità al fine di garantire la massima protezione dei dati attraverso il loro minimo trattamento;
- provvede a formare il personale sugli obblighi in materia di protezione dei dati personali in relazione alle specifiche competenze rivestite dai singoli dipendenti e dai rispettivi uffici in cui sono inseriti.

Art. 21

D.P.I.A.

1. Oltre le misure preventive di cui all'articolo precedente, l'Ente quando un trattamento presenta a seguito di analisi, rischi elevati per i diritti e le libertà degli interessati, procede alla valutazione di impatto sulla protezione dei dati (D.P.I.A.).

Art. 22

Procedimento

1. Qualora ricorra un rischio elevato il Titolare del trattamento, chiede il parere del Responsabile della Protezione dei dati e, se lo ritiene opportuno, degli stessi interessati.

2. La D.P.I.A. deve presentare il seguente contenuto minimo:

- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi.

Art. 23

Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici

1. Il Titolare del trattamento insieme al Responsabile della sicurezza informatica e al Responsabile della Protezione dei dati, controlla le banche dati organizzate in archivi elettronici e fornisce a tutto il personale che le utilizza direttive per garantire che le operazioni informatiche di trattamento siano svolte senza rischi per gli interessati. In particolare vengono adottate le seguenti misure di sicurezza:

- attribuzione agli incaricati di codici identificativi (parola chiave) composti di almeno otto caratteri, oppure, nel caso lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito; la stessa andrà modificata almeno ogni tre/sei mesi;
- disattivazione dei codici identificativi in caso di perdita della qualità degli stessi o di mancato utilizzo per un periodo superiore a sei mesi;
- uso ed aggiornamento del software antivirus, almeno con cadenza semestrale/mensile/quindicinale;
- sistemi antintrusioni e di protezione (firewall, antivirus ecc.), misure antincendio;
- sistemi di copiatura e conservazione di archivi elettronici, misure idonee a ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.

Art. 24

Misure per dati raccolti con sistemi di videosorveglianza

1. 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.

2. Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando – quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.

TITOLO VI

DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

Art. 25

Definizione di violazione dati personali

1. La violazione dei dati personali è una violazione di sicurezza che comporta accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali.

2. Per **distruzione non autorizzata** è da intendersi un'azione che rende irreversibile il processo di ricostruzione del dato personale determinando la sua esatta e totale eliminazione in rerum natura.

3. Per **perdita** è da intendersi la fuoriuscita del dato trattato ai fini di privacy dalla sfera del legittimo detentore in modo del tutto incontrollato e non tracciato.

4. Per **modifica non autorizzata** è da intendersi una deficienza organizzativa o fatti illeciti che, incidendo sulla conformazione del dato, è capace di arrecare danni fisici e morali agli interessati

Art. 26

Procedimento in caso di data breach

1. Il Responsabile del trattamento in caso venga a conoscenza della violazione informa senza ingiustificato ritardo il Titolare del trattamento e richiede immediato parere al Responsabile della protezione dei dati sulla gravità della violazione, ovvero:

- se questa sia inoffensiva per le misure di sicurezza già presenti in questo ente;
- se può comportare rischi per gli interessati al trattamento ed il grado dei rischi;
- le misure di sicurezza eventualmente da adottare per porre rimedio alla violazione.

2. Al Titolare del trattamento compete la valutazione finale sulla gravità o meno della violazione. In caso venga riscontrata la presenza di rischi per le persone fisiche va effettuata via Pec la notifica del data breach al Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza.

Art. 27***Notifica al Garante della privacy***

1. La Notifica al Garante non è necessaria se la violazione è inoffensiva, cioè vi è assenza di rischio per interessati e persone fisiche e ciò si verifica se l'Ente al momento in cui essa si è verificata aveva misure di sicurezza che hanno reso i dati inintelligibili perché per esempio anonimi o cifrati in modo sicuro.

Art. 28***Comunicazione all'interessato***

1. Il Titolare del trattamento comunica, senza giustificato ritardo, all'interessato la violazione in presenza solo di rischio elevato per i diritti e le libertà delle persone fisiche. Quanto più attuale è il dato violato tanto maggiore è la probabilità di rischio elevato, intendendosi per attualità il tempo trascorso dall'acquisizione/raccolta del dato.

2. La comunicazione all'interessato va effettuata con un linguaggio semplice e chiaro e deve presentare anch'essa un contenuto minimo rappresentato da:

– il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; le probabili conseguenze della violazione dei dati personali

TITOLO VII**ENTRATA IN VIGORE****Art. 29*****Abrogazioni***

1. Il presente regolamento modifica qualunque altra disposizione concernente la materia precedentemente approvata; per quanto non previsto si applicano direttamente le norme del regolamento europeo.

2. Il presente regolamento fa riferimento alle sole norme del Codice della privacy ancora oggi vigenti.

Art. 30***Entrata in vigore del regolamento***

1. Il presente regolamento entra in vigore il giorno in cui diviene esecutivo attraverso ordine di servizio.