

Allegato alla Delibera n. 15 del 27/06/2024

Regolamento sulla gestione degli impianti di videosorveglianza installati presso Casa di Riposo Umberto I di Montebelluna

SOMMARIO:

1. PREMESSA E SCOPO	3
2. NORMATIVA DI RIFERIMENTO	3
3. DEFINIZIONI	3
4. CAMPO DI APPLICAZIONE	4
5. FINALITA' E PRINCIPI GENERALI	5
6. TUTELA DEI LAVORATORI	6
7. SOGGETTI	6
8. AREE SOGGETTE A RIPRESE	7
9. TIPOLOGIA E MODALITA' OPERATIVE DELLE RIPRESE	7
10. INFORMATIVA	8
11. PERIODO DI CONSERVAZIONE E CANCELLAZIONE DEI DATI	8
12. ACCESSO ALLA CONTROL ROOM	9
13. ACCESSO ALLE IMMAGINI SU MONITOR IN SUPPORTO DELLE ATTIVITÀ DI ASSISTENZA E CURA	9
14. ACCESSO ALLE IMMAGINI REGistrate	9
15. DIRITTI DELL'INTERESSATO	10
16. COMUNICAZIONE E DIFFUSIONE	12
17. PRIVACY BY DESIGN E BY DEFAULT E MISURE DI SICUREZZA	12
18. OBBLIGHI DEL RESPONSABILE ESTERNO DEL TRATTAMENTO	13
19. MANUTENZIONE DEGLI IMPIANTI	14
20. PROCEDURA PER L'INSTALLAZIONE DI NUOVI IMPIANTI DI VIDEOSORVEGLIANZA O SOSTITUZIONE DI QUELLI ESISTENTI	14
21. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ	14
22. ALLEGATI	16
a. Informativa integrale	16
b. Informativa breve	19
c. Modulo di istanza dell'interessato per accesso a videoregistrazioni	20
d. Modulo di richiesta interna di accesso alle videoregistrazioni	22
e. Nomina a Designato della videosorveglianza	23
f. Nomina ad Autorizzato della videosorveglianza	27
g. Nomina a Responsabile esterno con funzioni di Amministratore di Sistema	31
h. Informativa personale dipendente	37

PREMESSA E SCOPO

Ai sensi dell'art. 4 del Reg. UE 2016/679 (di seguito GDPR), la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini costituiscono tipologie di trattamento di dati personali. Possono infatti essere considerati dati personali tutte quelle informazioni relative ad una persona fisica identificata o identificabile.

Conseguentemente, anche i sistemi di videosorveglianza rappresentano una forma di trattamento di dati personali (dati dei soggetti che lavorano presso la struttura, a favore della stessa ovvero si avvalgano dei servizi prestati dall'Ente) che necessita di conformarsi alla normativa vigente in ambito privacy.

Inoltre, in base a specifiche disposizioni dell'ordinamento, suddetti sistemi dovranno rispettare anche altre normative quali, ad esempio, le norme riguardanti il controllo a distanza dei lavoratori, disciplinato dall'art. 4 della Legge 300/1970 e s.m.i.

Alla luce delle disposizioni sopra citate, codesto Ente, con il presente documento, intende disciplinare l'utilizzo dei sistemi di videosorveglianza installati presso tutte le sedi dell'Ente, nel rispetto dei diritti e delle libertà fondamentali degli interessati nonché della dignità delle persone fisiche con particolare riferimento alla riservatezza, all'identità personale.

Il regolamento è pubblicato nella intranet aziendale ed è consegnato ai responsabili esterni in fase di stipula del contratto.

NORMATIVA DI RIFERIMENTO

La normativa di riferimento per la stesura del presente documento è la seguente

Regolamento Europeo 679/2016	Regolamento generale sulla protezione dei dati
D.lgs. n.196/2003 e s.m.i.	Codice in materia di protezione di dati personali
Provvedimento del Garante per la Protezione dei Dati Personali – 8 aprile 2010	Provvedimento emanato dall'autorità Garante della privacy per le corrette modalità di utilizzo degli impianti di videosorveglianza
L. 300/1970 s.m.i.	Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento
D. lgs 81/2008 s.m.i.	Testo Unico in materia di salute e sicurezza nei luoghi di lavoro

DEFINIZIONI

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di

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

Videosorveglianza: sistema o dispositivo che permette la visione e la registrazione di immagini.

Videocontrollo: sistema o dispositivo che permette unicamente la visione in tempo reale delle immagini.

Impianti audiovisivi: strumenti che permettono sia la visione di immagini sia l'ascolto di suoni.

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati particolari: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile esterno del trattamento: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali.

Designato: la persona fisica autorizzata non solo a compiere operazioni di trattamento dal Titolare ma che visualizza le immagini registrate e gestisce le modalità di utilizzo interno dell'impianto.

Autorizzato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Designato.

Interessato: la persona fisica, cui si riferiscono i dati personali.

Nel presente Regolamento, ove non diversamente specificato, il termine "videosorveglianza" viene utilizzato genericamente al fine di ricomprendere sia la videosorveglianza in senso stretto che il videocontrollo.

CAMPO DI APPLICAZIONE

Il presente regolamento si applica:

- al personale preposto al trattamento dei dati personali tramite il sistema di videosorveglianza, specificamente autorizzati, ovvero ai delegati privacy per la Videosorveglianza;
- alla società nominata responsabile esterna del trattamento ai sensi dell'art. 28 del GDPR.

FINALITA' E PRINCIPI GENERALI

Gli impianti di videosorveglianza, installati presso le strutture dell'Ente, hanno esclusivamente il fine di garantire:

- A. La tutela del patrimonio dell'Ente da possibili furti, rapine, danneggiamenti, atti di vandalici o eventi simili;
- B. La sicurezza e l'incolumità dei lavoratori e dei visitatori all'interno delle strutture;
- C. Implementazione dei sistemi di incolumità e assistenza degli ospiti del Nucleo Alzheimer;

Le telecamere, per le finalità di cui A-C, sono state installate nei punti indicati nell'allegato al presente regolamento.

Il sistema di videosorveglianza, in ogni caso, è stato progettato nel rispetto dei diritti e delle libertà fondamentali, della dignità degli interessati nonché in aderenza ai principi fondamentali stabiliti dal Regolamento UE 2016/679 e dal Garante della Privacy, come di seguito riportati.

L'Ente assume l'impegno a non utilizzare per finalità differenti le riprese effettuate. I sistemi di videosorveglianza in uso escludono il controllo a distanza dell'attività dei lavoratori.

Principio di Liceità

Il trattamento dei Dati attraverso il sistema di videosorveglianza avviene nel rispetto dei presupposti di liceità di cui all'art. 6 paragrafo 1 lett. c) ed e) del GDPR.

Principio di finalità

Ai sensi dell'art. 5 paragrafo 1 lett. b) i dati sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità.

Principio di correttezza e trasparenza

Il trattamento viene effettuato in modo corretto e trasparente nei confronti degli interessati.

Principio di minimizzazione/necessità

I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattate in base all'art. 5 paragrafo 1 lett. c) del GDPR. Inoltre, i sistemi di videosorveglianza ed i sistemi/programmi informatici utilizzati sono configurati al fine di ridurre al minimo l'utilizzazione di dati personali di modo da escludere il trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi o modalità che permettano l'identificazione unicamente in caso di necessità.

Principio di Proporzionalità

L'attività di videosorveglianza deve essere proporzionale agli scopi perseguiti.

In applicazione di tale principio, nel bilanciamento tra le esigenze di videosorveglianza ed il rischio concreto va evitata la rilevazione di dati in aree non soggette a concreti pericoli o per le quali non sussiste alcuna esigenza giustificativa. Conseguentemente, tale principio dovrà essere considerato nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento.

Inoltre, gli impianti di videosorveglianza possono essere adottati unicamente nelle ipotesi in cui altri sistemi risultino inefficaci rispetto alle finalità perseguite.

TUTELA DEI LAVORATORI

Come esplicitato nelle premesse, l'utilizzazione di sistemi di videosorveglianza potrebbe produrre un controllo seppur occasionale del personale dell'Ente.

Per tale motivo, l'attività di videosorveglianza deve essere svolta nel rispetto, oltre che delle disposizioni in materia di protezione dei dati personali e del provvedimento del Garante della privacy del 8 aprile 2010, anche dello Statuto dei Lavoratori al fine di salvaguardare i dipendenti da forme di controllo a distanza sul loro operato.

Conseguentemente, laddove dai sistemi di Videosorveglianza derivi la possibilità di un controllo a distanza del personale, l'Ente adotta le garanzie previste dall'Art. 4 dello Statuto dei Lavoratori sottoponendo al vaglio delle rappresentanze sindacali e/o dell'Ispettorato del Lavoro gli impianti.

Le riprese video riguarderanno i luoghi in cui transitano o operano i lavoratori limitatamente a quanto strettamente indispensabile per il raggiungimento degli scopi sopradescritti, escludendo aree quali bagni, spogliatoi o zone adiacenti a rilevatori marcatempo.

Inoltre, l'Ente non utilizzerà le riprese né per controllare l'attività del personale né per adottare nei suoi confronti comportamenti discriminatori, sanzioni disciplinari o richiedere risarcimenti, salvo le ipotesi di comportamenti illeciti per i quali è previsto l'intervento delle autorità di pubblica sicurezza e/o giudiziarie.

I dipendenti sono stati informati circa le modalità di utilizzo del sistema di videosorveglianza e la presenza delle telecamere nonché del relativo posizionamento, previo rilascio di informativa privacy, ai sensi del Regolamento Europeo 679/2016.

SOGGETTI

Titolare del Trattamento

Il Titolare del Trattamento dei dati raccolti con i sistemi di videosorveglianza è l'Ente nella persona del suo legale rappresentante pro tempore. Il Titolare ha la responsabilità di garantire che l'utilizzo dei sistemi di Videosorveglianza avvenga nel rispetto della normativa vigente.

Il responsabile della protezione dei dati

Il responsabile della protezione dei dati (RPD o DPO) è una figura prevista dal Regolamento UE 2016/69. Si tratta di un soggetto designato dall'Ente con funzioni consultive, formative e di vigilanza relativamente all'applicazione del Regolamento sopracitato. Tale soggetto può essere contattato ai seguenti recapiti _____.

Designato/i privacy per la Videosorveglianza

Il Designato privacy per la Videosorveglianza è incaricato, sulla base della designazione ricevuta nonché delle istruzioni impartitegli dal Titolare, a gestire il trattamento dei dati personali raccolti per il tramite di sistemi di videosorveglianza nonché a sovrintendere all'attività degli incaricati e dei responsabili esterni con riferimento al sopracitato trattamento.

Egli, inoltre, provvederà alla tenuta di un registro degli accessi alle immagini registrate.

Per ogni struttura ove è presente un sistema di videosorveglianza viene nominato un designato.

Autorizzati al trattamento dei dati derivanti dai sistemi di Videosorveglianza

Gli Autorizzati al trattamento dei dati derivanti dai sistemi di Videosorveglianza vengono nominati mediante atto scritto del Titolare nel quale viene specificato l'ambito del trattamento demandato a ciascuno (sola visione delle immagini in diretta, accesso alle immagini registrate, estrazione di copia delle immagini e/o manutenzione delle apparecchiature e dei software di gestione).

Tali soggetti, all'esito della nomina ma prima di operare qualsivoglia trattamento sulle immagini, saranno istruiti sul corretto uso degli strumenti di videosorveglianza e sulla normativa di riferimento. Gli autorizzati svolgeranno la propria attività nel rispetto dei profili di autorizzazione e delle istruzioni operative impartite nell'atto di nomina nonché attenendosi a quanto ivi previsto.

Responsabili esterni del trattamento.

Il Titolare del trattamento può avvalersi di soggetti esterni all'Ente per la gestione/assistenza/manutenzione dei sistemi di Videosorveglianza. In tali casi il Titolare provvederà a disciplinare i trattamenti da parte dei Responsabili mediante contratto ai sensi dell'art. 28 del Regolamento UE 2016/679 con la qualifica di amministratori di sistema.

AREE SOGGETTE A RIPRESE

Le aree sottoposte a videosorveglianza sono quelle ritenute strettamente indispensabili al perseguimento delle finalità sopra citate. Le stesse sono segnalate da apposita cartellonistica contenente un'informativa di primo livello ai sensi di quanto disposto dal Reg UE 2016/679.

Al fine di identificare la precisa ubicazione delle telecamere nonché il loro angolo di ripresa, si rimanda alle planimetrie allegate. Rimane inteso che il Titolare potrà apportare delle modifiche e/o variazioni – qualitative e/o quantitative- nel rispetto delle finalità già enunciate.

TIPOLOGIA E MODALITA' OPERATIVE DELLE RIPRESE

La raccolta dei dati avviene tramite telecamere aventi le caratteristiche tecniche (sistema di autenticazione, misure di sicurezza specifiche, caratteristiche generali delle telecamere) descritte in appositi documenti allegati al presente.

Le tipologie di sorveglianza effettuate si possono distinguere in:

- riprese senza registrazione (e, dunque, con sola visione delle immagini);
- riprese con registrazione di immagini.

Ad ogni modo:

- le telecamere sono posizionate in modo da raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità sopradescritte;
- la localizzazione delle telecamere e delle modalità di ripresa sono determinate in ottemperanza a quanto sopraindicato;
- l'angolo e la panoramica sono tali da limitare la videosorveglianza alle sole aree interessate dalle finalità dell'impianto;
- i monitor degli impianti installati per le finalità di cui ai nn. 1-2-3 sono collocati esclusivamente nei locali di ogni struttura denominati "control room", dove l'accesso è interdetto salvo ai soggetti espressamente autorizzati in conformità al presente Regolamento;
- i monitor in supporto delle attività di assistenza e cura di cui alla finalità 4 sono collocati in un locale (control room) dove non è permesso accesso a persone estranee al percorso assistenziale e/o di cura, salvo le ipotesi previste dal presente Regolamento.
- le telecamere non sono dotate di sistemi di rilevazione audio;
- gli impianti sono in funzione in modalità continuata nelle 24 ore;
- sono esclusi software con funzionalità di video-analisi "intelligenti".

INFORMATIVA

L'Ente informa gli interessati in ordine alla presenza di aree sottoposte a videosorveglianza mediante l'affissione di idonea cartellonistica.

La suddetta informativa breve dovrà essere collocata prima del raggio di azione delle videocamere, anche nelle loro immediate vicinanze e non necessariamente a contatto le telecamere.

I singoli cartelli dovranno essere tali da risultare ben visibili, sia con riferimento al formato che alla collocazione, anche in condizioni di scarsa illuminazione ambientale ed anche in ipotesi di attivazione del sistema di videosorveglianza in orario notturno.

Inoltre, l'Ente, mediante idonei strumenti (quali il sito aziendale e/o l'affissione in bacheca) mette a disposizione degli interessati l'informativa estesa.

Tutto il personale è stato informato dell'adozione del sistema di videosorveglianza mediante informativa scritta.

Copia del Regolamento completo è a disposizione di tutto il personale, presso la sede aziendale.

PERIODO DI CONSERVAZIONE E CANCELLAZIONE DEI DATI

Le immagini registrate dalle telecamere, saranno conservate, su appositi server o supporti analoghi, e nel rispetto delle misure di sicurezza richieste dalla normativa vigente, per un periodo di 168 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in caso di festività o chiusura degli uffici. In tali ultime ipotesi, il tempo di conservazione verrà esteso fino a 168 ore.

Solo per aderire a specifiche richieste delle Autorità giudiziarie e/o di polizia sarà possibile superare suddetti limiti e ciò fino al tempo utile per le autorità di acquisire copia delle riprese.

Inoltre, in casi eccezionali, in relazione a particolari esigenze tecniche o situazioni di grave rischio (debitamente valutate unitamente al DPO) è ammesso il salvataggio di immagini relative a ben definiti periodi e luoghi di ripresa in attesa della richiesta delle Autorità Giudiziarie o al fine di adempiere a specifiche richieste di accesso da parte di soggetti legittimati. In quest'ultimo caso,

saranno messe a disposizione unicamente le immagini pertinenti alla richiesta di accesso e verrà limitata ogni altra visione.

I sistemi di videosorveglianza sono programmati in modo da operare, allo scadere del tempo di conservazione prefissato, l'integrale cancellazione automatica dei dati, anche mediante sovra registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

ACCESSO ALLA CONTROL ROOM

L'accesso alla control room è consentito unicamente ai Designati e a soggetti autorizzati, nonché ai tecnici addetti all'assistenza e alla manutenzione degli impianti limitatamente a quanto strettamente necessario con riferimento alle mansioni loro affidate e nei limiti delle autorizzazioni rilasciate.

L'eventuale accesso di soggetti terzi, giustificato da necessità manutentive (ad es. tecnici di impianti di areazione, idraulici e/o elettrici, ...), sarà specificamente autorizzato dal designato e, in ogni caso, sottoposto alla supervisione degli autorizzati.

ACCESSO ALLE IMMAGINI SU MONITOR IN SUPPORTO DELLE ATTIVITÀ DI ASSISTENZA E CURA

L'accesso alle immagini proiettate sui monitor in supporto delle attività di assistenza e cura di cui alla finalità C è permesso unicamente al personale, all'uopo autorizzato, che si occupa del percorso assistenziale e/o di cura.

Qualora vi sia la necessità di permettere la visione dei monitor da parte di soggetti diversi (per es. familiari del paziente che non possono accedere alla stanza ove lo stesso è ricoverato, responsabili esterni per attività di manutenzione), questi ultimi saranno specificamente autorizzati dal Designato e potranno accedere alle sale unicamente se accompagnati da personale autorizzato. In tali casi, la visione sarà limitata ai soli monitor di rilevanza per il soggetto.

ACCESSO ALLE IMMAGINI REGISTRATE

L'accesso alle immagini registrate è consentito, nell'arco temporale stabilito dai termini di conservazione ed al solo scopo di conseguire le finalità sopracitate, unicamente ai soggetti di seguito elencati.

- a. Al Titolare, nella persona del Suo legale rappresentante *pro tempore*, al Designato privacy per la Videosorveglianza e, nei limiti delle operazioni di loro competenza, agli Autorizzati al trattamento dei dati derivanti dai sistemi di Videosorveglianza;
- b. Ai responsabili esterni del trattamento limitatamente a quanto necessario per lo svolgimento delle attività loro demandate;
- c. All'interessato del trattamento, poiché ripreso dal sistema di Videosorveglianza, previa presentazione e relativo accoglimento della richiesta dallo stesso presentata ai sensi del GDPR.. In tale ipotesi l'accesso sarà limitato alle sole immagini che riguardano direttamente il richiedente. Al fine, dunque, di evitare la visione di immagini ritraenti soggetti diversi, il Titolare dovrà provvedere a schermare il video ovvero a adottare altri accorgimenti tecnici che impediscano l'identificazione di altre persone fisiche eventualmente presenti;
- d. Ai soggetti legittimati all'accesso ai sensi della L. 241/1990 ed, in particolare, qualora

- l'accesso sia necessario per difendere interessi giuridici del richiedente. Anche in tale ipotesi si adotteranno le modalità di cui al punto c che precede per oscurare i soggetti la cui presenza non sia strettamente necessaria per la difesa degli interessi dell'istante;
- e. All'Autorità giudiziaria o di polizia ad esito di richieste investigative.

Tutti gli accessi alla visione saranno documentati mediante annotazione in un apposito registro denominato "registro degli accessi" contenente:

- Data ed ora dell'accesso;
- L'identificazione del terzo autorizzato;
- I dati per i quali si è svolto l'accesso;
- Gli estremi e la motivazione dell'autorizzazione all'accesso;
- Le modalità di accesso (es. mera visualizzazione o estrazione di copia);
- La sottoscrizione del medesimo.

Tale registro è tenuto e conservato dal Designato.

Il Titolare del trattamento o il Designato possono segnalare la necessità/opportunità di accedere alle registrazioni, per le finalità sopracitate, mediante la compilazione del modulo allegato contenente tutti gli elementi atti a circoscrivere la richiesta.

La richiesta andrà trasmessa ad un addetto specificamente autorizzato ad estrapolare le immagini/riprese. Se necessario, quest'ultimo provvederà ad oscurare le immagini relative a soggetti estranei all'evento. Potranno essere, tuttavia, estrapolati anche tali dati nell'ipotesi in cui la scomposizione o l'esclusione di taluni loro elementi renda incomprensibili i dati richiesti.

Tali immagini verranno visionate preventivamente dal Designato e, se del caso, dal referente privacy aziendale, al fine di vagliare il rispetto del principio di minimizzazione (in caso contrario le immagini dovranno essere ulteriormente elaborate) e l'eventuale necessità di coinvolgere le autorità giudiziarie competenti.

Al fine di evitare la cancellazione automatica dei dati così estratti, essi verranno conservati, in formato elettronico/cartaceo e adottando le misure idonee al fine di garantire una corretta conservazione, per il tempo necessario a consentire l'acquisizione delle stesse da parte dell'Autorità pubblica competente.

In presenza di una formale richiesta delle Autorità giudiziarie o di polizia, le immagini saranno consegnate e verranno distrutte eventuali copie esistenti.

DIRITTI DELL'INTERESSATO

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in conformità alle disposizioni del GDPR, ha diritto:

- a) di ottenere dal titolare del trattamento 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 stessi;
- b) di essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;

c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.

L'istanza per l'esercizio dei diritti dell'interessato è presentata direttamente al Titolare oppure al Responsabile della Protezione dei dati.

Nel caso di richiesta di accesso alle immagini registrate, l'interessato dovrà provvedere ad indicare elementi atti a permettere una facile individuazione delle immagini richieste quali, a titolo esemplificativo:

- il luogo e la fascia oraria della possibile ripresa;
- l'abbigliamento o accessori indossati al momento della possibile ripresa;
- l'eventuale presenza di accompagnatori al momento della possibile ripresa;
- l'eventuale attività svolta al momento della possibile ripresa.

Ricevuta la richiesta, l'Ufficio preposto ne valuterà le motivazioni a sostegno e, qualora il Designato ritenga di dover evadere la richiesta e riscontri la presenza effettiva delle immagini, trasmetterà la stessa ad un autorizzato al fine di permettere l'estrapolazione delle immagini. Tale estrapolazione dovrà essere limitata il più possibile alle immagini che riguardano unicamente l'interessato.

Contestualmente, verrà fissato un appuntamento in occasione del quale l'interessato potrà prendere visione delle immagini che lo riguardano ed eventualmente chiederne copia. Rimane inteso che le immagini di cui l'interessato potrà prendere visione e/o ottenerne copia, dovranno essere debitamente oscurate al fine di tutelare la privacy di eventuali soggetti terzi.

Qualora sia necessario che filmato integrale non subisca l'automatica cancellazione, esso verrà conservato per il tempo necessario a permettere all'interessato di rivolgersi all'autorità pubblica competente per vedere tutelati i propri diritti/interessi.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Inoltre, nell'esercizio dei diritti l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

COMUNICAZIONE E DIFFUSIONE

La comunicazione a soggetti pubblici dei dati personali acquisiti mediante i sistemi di videosorveglianza è ammessa solo se prevista da norma di legge o, nei casi previsti dalla legge, di regolamento.

In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali, previa comunicazione al Garante secondo quanto previsto dall'art. 2-ter, comma 2, del D.Lgs. n. 196/2003. Rimane impregiudicata la possibilità di comunicare o diffondere i dati qualora vi sia una richiesta, in conformità alla legge da parte di forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D. Lgs. n. 196/2003 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

La comunicazione e la diffusione avverranno, in ogni caso, previa autorizzazione del Titolare e non si effettuerà in alcun caso una diffusione generalizzata.

PRIVACY BY DESIGN E BY DEFAULT E MISURE DI SICUREZZA

I dati personali sono protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio.

In particolare, il Titolare garantisce:

- a) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi;
- b) il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente;
- c) la periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative adottate.

Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, l'Ente terrà in considerazione i rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trattati dal Titolare.

A questo fine, sono adottate le seguenti specifiche misure tecniche e organizzative:

- a) per quanto riguarda il periodo di conservazione delle immagini, sono predisposte misure per la cancellazione automatica delle registrazioni allo scadere del termine previsto;
- b) gli apparati connessi a reti informatiche dovranno essere protetti contro i rischi di accesso abusivo;
- c) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza sarà effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless;
- d) la rete informatica è dotata di antivirus e firewall a protezione da attacchi esterni;
- e) non vengono effettuati collegamenti da remoto al sistema di videosorveglianza o alle immagini registrate, attraverso reti pubbliche di comunicazione;

Ulteriori specifiche sono disponibili nel manuale d'uso del sistema.

Inoltre, Il Titolare ed il Designato vigilano sulla condotta di coloro che agiscono sotto la loro autorità, provvedendo, tra l'altro, alla loro adeguata formazione circa le finalità e modalità del trattamento, le corrette misure per l'accesso ai sistemi e gli obblighi di custodia dei dati.

Infine, si segnala che l'apparato di videosorveglianza presenta un sistema di autorizzazione che prevede il controllo degli accessi effettuati per visionare le registrazioni mediante username e password con scadenza periodica e cambio in autonomia delle credenziali.

Inoltre, il sistema di autorizzazione prevede la presenza di diversi profili di autorizzazione all'accesso alle immagini:

- I. Operator: accesso in sola visualizzazione
 - II. Supervisor: accesso sia in visualizzazione che in registrazione
 - III. Administrator: accesso in visualizzazione, in registrazione e modifica configurazione di sistema.
- l'accesso alle immagini registrate sarà tracciato mediante log, al fine di monitorare eventuali accessi non autorizzati.
 - Le credenziali di autenticazione, che consentono l'accesso alle immagini, saranno conservate in busta chiusa e sigillata, in area riservata, la quale sarà aperta solo nei casi e per le finalità indicate. Sarà quindi adottato un sistema per la gestione delle password, in modo da limitare l'accesso al sistema di videosorveglianza, anche al personale autorizzato.
 - È stata predisposta una busta sigillata con relativa password per ogni profilo di autorizzazione.
 - Eventuali richieste di apertura della busta per accesso alle immagini saranno registrate su modulo opportunamente predisposto.

OBBLIGHI DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

Il responsabile esterno del trattamento deve garantire l'adozione di misure tecniche e organizzative adeguate in particolare al fine di assicurare, per impostazione predefinita, che i dati non siano resi accessibili ad un numero indefinito di persone (es. tramite credenziali di accesso).

Inoltre, egli è tenuto ad adempiere agli obblighi di cui al GDPR (cfr. artt. 32, 33, 34, 35, 36) e, in particolare, a:

- Adottare e documentare l'adozione di misure tecniche ed organizzative tali da garantire il rispetto della normativa vigente;
- Adottare e documentare, per i sistemi di videosorveglianza e nello svolgimento dei servizi allo stesso affidati, l'adozione delle misure di sicurezza richieste dall'art. 32 del GDPR, tenendo conto della natura dei dati e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- Informare il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione dei dati o di incidenti che posano impattare in modo significativo sui dati personali;
- Assistere il titolare nel garantire il rispetto degli obblighi previsti dagli artt. 32, 33, 34, 35, 36

del GDPR;

- Garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiamo un adeguato obbligo legale di riservatezza.

MANUTENZIONE DEGLI IMPIANTI

Le società incaricate di effettuare opere di manutenzione/revisione dei sistemi di videosorveglianza – all'uopo nominate responsabili esterne del trattamento - potranno accedere ai sistemi di registrazione tramite specifiche credenziali prive di abilitazione alla visione delle immagini.

Qualora sia necessario operare degli interventi di manutenzione sui sistemi di videosorveglianza che implichino l'accesso alle immagini da parte degli addetti alla manutenzione, sarà possibile unicamente se esso risulta indispensabile all'espletamento dell'attività manutentive e comunque sempre in presenza di soggetti incaricati dotati delle credenziali di autenticazione abilitate alla visione delle immagini.

Le sopracitate società, inoltre, dovranno custodire un registro denominato "registro degli interventi" in cui annotare, per ogni intervento effettuato, le seguenti informazioni:

- Data di accesso;
- Nominativo e/o codice identificativo dell'operatore

PROCEDURA PER L'INSTALLAZIONE DI NUOVI IMPIANTI DI VIDEOSORVEGLIANZA O SOSTITUZIONE DI QUELLI ESISTENTI

Nel caso di installazione di nuovi impianti o di sostituzione/modifica di quelli esistenti, dovrà essere seguita la procedura sotto riportata:

- La richiesta dovrà essere adeguatamente motivata ed in linea con il principio di proporzionalità;
- La richiesta andrà indirizzata all'ufficio della Direzione, che attiverà la procedura interna sia da un punto di vista tecnico-patrimoniale che dei diritti dei soggetti interessati;
- Ad esito di tale procedura, la richiesta verrà sottoposta all'organo decisionale competente.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Titolare del Trattamento: Casa di Riposo Umberto I nella persona del legale rappresentante *pro tempore*

Responsabile Esterno del Trattamento dei Dati Personali: se nominato

Autorizzato alla Custodia delle copie delle credenziali e chiavi di accesso:

Autorizzato alla Custodia delle Aree e dei Locali:

Designati del Trattamento dei Dati Personali:

Autorizzati al trattamento:

✓

(visualizzazione e registrazioni)

ALLEGATI

a. Informativa integrale

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI CONNESSI AL'USO DELL'IMPIANTO DI VIDEOSORVEGLIANZA AI SENSI DEL REGOLAMENTO UE 2016/679 (GDPR)

Ai sensi di quanto disposto in materia di protezione dei dati personali dalla normativa vigente, Casa di Riposo Umberto I in qualità di Titolare del Trattamento dei dati, informa che presso le sedi di Montebelluna è in funzione un sistema di videosorveglianza tramite telecamere. La gestione e l'utilizzo di tale sistema avviene in conformità con il GDPR, nonché con il Codice della Privacy (D.Lgs. 196/2003) come modificato dal D.Lgs. 101/2018 e con il Provvedimento del Garante della Privacy dell'8 aprile 2010

La presente informativa integra l'informativa "semplificata" fornita da codesto Titolare per il tramite della cartellonistica affissa in prossimità delle telecamere.

Titolare del Trattamento

Casa di Riposo Umberto I con sede legale in Montebelluna, tel 0423 2871, mail info@umbertoprino.com, PEC posta@pec.umbertoprino.com in persona del legale rappresentante *pro tempore*.

Responsabile della protezione Dati

Il Responsabile della protezione Dati è reperibile ai seguenti recapiti: tel. 049 0998416; e-mail: dpo@robbyone.net; pec: dpo.robbyone@ronepec.it

Informazioni sui dati raccolti

I dati personali che La riguardano, raccolti e trattati dal Titolare del trattamento, sono le immagini rilevate attraverso il sistema di videosorveglianza attualmente in uso.

Finalità trattamento

- D. La tutela del patrimonio dell'Ente da possibili furti, rapine, danneggiamenti, atti di vandalici o eventi simili;
- E. La sicurezza e l'incolumità dei lavoratori e dei visitatori all'interno delle strutture;
- F. Implementazione dei sistemi di incolumità e assistenza degli ospiti del Nucleo Alzheimer;

Base giuridica del trattamento

La base giuridica del trattamento è data dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'art.

6, paragrafo 1, lettera e, del Regolamento UE 2016/679 e dalla necessità di adempiere un obbligo legale al quale è soggetto il titolare del trattamento ai sensi dell'art. 6, paragrafo 1, lettera c, del Regolamento UE 2016/679 (DGR 84/2007).

.

Categorie destinatari dei dati

I Suoi dati saranno comunicati ai dipendenti e collaboratori del Titolare che operano in qualità di autorizzati al trattamento in ragione del proprio profilo.

I Suoi dati, inoltre, potranno essere comunicati a persone, fisiche o giuridiche, che collaborano con il titolare per il perseguimento delle sopracitate finalità. Tali soggetti svolgeranno la funzione di responsabili esterni del trattamento ai sensi dell'art. 28 del Regolamento oppure opereranno come autonomi titolari del trattamento.

Le immagini non saranno in alcun modo comunicate o divulgate a terzi se non per rispondere ad eventuali richieste da parte dell'Autorità Giudiziaria o degli Organi di Polizia.

Periodo di conservazione dei dati ed eventuale trasferimento dei dati all'estero

Le immagini riprese dal sistema di videosorveglianza verranno conservate per 168 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa. Dopo tale periodo, si provvederà alla cancellazione delle stesse mediante sovrascrittura.

I dati personali non saranno trasferiti ad un paese terzo o ad un'organizzazione internazionale.

Esistenza di processi decisionali automatizzati: No.

Modalità del trattamento

Il trattamento dei Suoi dati avverrà nel rispetto del principio di liceità, correttezza, trasparenza, adeguatezza, pertinenza, e necessità di cui all'art. 5, paragrafo 1, del Regolamento UE, mediante strumenti manuali, informatici e telematici in modo pertinente e limitato a quanto necessario rispetto alle finalità e, comunque, in modo da garantire la massima sicurezza e riservatezza e sempre in piena conformità alla normativa vigente.

Diritti degli Interessati

Lei potrà, in qualsiasi momento, esercitare i diritti:

- di accesso ai dati personali (art. 15 del GDPR)
- di ottenere la cancellazione degli stessi o la limitazione del trattamento che lo riguardano (art. 16, 17 e 18 del GDPR);
- di opporsi al trattamento dei dati (art. 21 del GDPR);
- alla portabilità dei dati (art. 20 del GDPR).

Trattandosi di dati trattati tramite il sistema di videosorveglianza non è in concreto esercitabile il diritto di rettifica in quanto si tratta di immagini raccolte in tempo reale.

L'esercizio dei suoi diritti potrà avvenire attraverso l'invio di una richiesta cartacea o a mezzo mail al Titolare del Trattamento ovvero al responsabile della protezione dei dati.

L'interessato ha, in ogni caso, il diritto di proporre reclamo all'autorità di controllo (Garante Privacy)

(art. 15, par. 1, lett. *f*).

b. Informativa breve

L'informativa breve¹ dovrà contenere le seguenti informazioni:

- L'identità del titolare e i dati di contatto;
- I riferimenti del DPO;
- Le finalità;
- La base giuridica del trattamento;
- La presenza di eventuali registrazioni delle immagini e il tempo della loro conservazione;
- I diritti degli interessati;
- L'indicazione del luogo (cartello in reception, documento nel sito istituzionale, ...) ove sia possibile reperire l'informativa estesa;
- Eventuale qrcode.

ESEMPIO



VIDEOSORVEGLIANZA

Titolare del Trattamento: RAGIONE SOCIALE, SEDE, RECAPITI
Responsabile della protezione dei dati: DATI DI CONTATTO

Indicare le caratteristiche più rilevanti ad es: periodo di conservazione o monitoraggio in tempo reale, diffusione o comunicazione a terzi

Finalità della videosorveglianza e base giuridica: ...

QR CODE

Ulteriori informazioni sono disponibili:
nell'avviso presente in reception, presso il punto informazioni sul sito

Diritti degli interessati: *gli interessati possono esercitare molteplici di ritti e in particolare possono richiedere l'accesso ai propri dati o la loro cancellazione.*

¹ Informativa tratta da *Guidelines 3/2019 on processing of personal data through video devices*, versione 2.0, adottata il 29 gennaio 2020 dall'*European Protection Board*.

c. Modulo di istanza dell'interessato per accesso a videoregistrazioni

Il/La sottoscritto/a,
nato/a a il
e residente in via/piazza
città provincia

PREMETTE

☐ essere transitato in area presumibilmente soggetta a riprese da parte del sistema di videosorveglianza dell'Ente

OPPURE

☐ aver subito/assistito a quanto di seguito descritto in un'area presumibilmente soggetta a riprese da parte del sistema di videosorveglianza dell'Ente

.....
.....
.....

Nella consapevolezza che le registrazioni del sistema di videosorveglianza vengono conservate per il tempo di 168 ore dalla ripresa e che, in presenza di motivata richiesta pervenuta prima del suddetto termine, le immagini (ove reperite) potranno essere estrapolate e custodite dal Titolare onde poter essere messe a disposizione dell'Autorità giudiziaria e/o di polizia

Tutto ciò premesso, il sottoscritto

CHIEDE

di esercitare il diritto di accesso alle immagini al seguente scopo:

☐ permettere l'acquisizione delle immagini da parte delle autorità giudiziarie/di polizia che indagano sui fatti sopradescritti

☐ altro

.....
.....
.....

Per permettere di individuare le immagini, si forniscono le seguenti informazioni:

1. Luogo/area di possibile ripresa
2. Data di possibile ripresae orario indicativo
3. Elementi utili ad individuazione del/della sottoscritto/a ad es. accessori, abbigliamento, attività svolta durante le riprese, ecc

.....
.....

-
.....
4. Presenza di altri soggetti (sommatoria descrizione)
-
.....
.....

Recapito/contatto per ulteriori approfondimenti

Luogo e data

Firma

d. Modulo di richiesta interna di accesso alle videoregistrazioni

Il/La sottoscritto/a,
ruolo

PREMETTE

di riscontrare l'esigenza di accedere alle immagini registrate perché (*specificare le ragioni della richiesta*):

.....
.....
.....

Per permettere di individuare le immagini, si forniscono le seguenti informazioni:

1. Luogo/area di possibile ripresa
2. Data di possibile ripresae orario indicativo
3. Elementi utili ad individuazione le immagini ad es. accessori, abbigliamento, attività svolta durante le riprese, ecc

.....
.....
.....
.....

4. Presenza di altri soggetti (sommara descrizione)

.....
.....
.....

Luogo e data

Firma

e. Nomina a Designato della videosorveglianza

NOMINA DI DESIGNATO AL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEGLI ARTICOLI 29 E 32 DEL REGOLAMENTO UE 2016/679 E DELL'ART.2 QUATERDECIES DEL CODICE PRIVACY

PREMESSO CHE

- Casa di Riposo Umberto I, in qualità di Titolare del Trattamento dei dati personali, è tenuto ad adempiere gli obblighi imposti dal Regolamento UE 2016/679 e dalla legislazione nazionale vigente (cfr. D.Lgs. 196/2003 e s.m.i.) sulla protezione dei dati personali.
- Con riferimento a tali obblighi, il Titolare del Trattamento è tenuto ad adottare specifiche misure tecnico - organizzative oltre ad impartire specifiche istruzioni al proprio personale.
- Nella gestione dei dati personali, Casa di Riposo Umberto I intende avvalersi delle figure dei Designati del Trattamento dei dati con il compito di coadiuvare il Titolare del Trattamento nell'adempimento degli obblighi di alla normativa.

Tutto ciò premesso e considerato,

in virtù dell'attività direzionale svolta da _____ all'interno dell'Ente, nonché dell'esperienza e della capacità maturate nel mettere in atto le misure tecniche ed organizzative adeguate al fine di garantire la tutela dei diritti dell'interessato,

il Titolare nomina

DESIGNATO PRIVACY PER I TRATTAMENTI DI DATI PERSONALI E PARTICOLARI REALIZZATI PRESSO L'AREA _____ NONCHE' DI QUELLI DERIVANTI DAL SISTEMA DI VIDEOSORVEGLIANZA

Alla luce della presente nomina Lei è tenuto all'osservanza delle disposizioni vigenti nell'ambito della tutela dei dati personali nonché delle istruzioni operative sotto riportate.

Le ricordiamo che, in base ai principi enunciati dall'art. 5 del Regolamento UE 2016/679, i dati dovranno essere:

- 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 («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («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 («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 («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 («integrità e riservatezza»).

Le precisiamo, inoltre, che il Titolare è tenuto ad osservare e comprovare il rispetto dei predetti principi e, conseguentemente Lei, in qualità di Designato, dovrà essere in grado di provare che nell'Area di gestione a Lei affidata, inclusa l'attività di gestione del sistema di videosorveglianza, siano state adottate adeguate misure tecnico-organizzative al fine della completa aderenza al Regolamento Europeo e alla normativa nazionale vigente in materia.

COMPITI ED ISTRUZIONI OPERATIVE NELLA GESTIONE DEI DATI PERSONALI DA PARTE DEL DESIGNATO

Il designato al trattamento dei dati personali dovrà:

- accedere ai sistemi informatici di Casa di Riposo Umberto I unicamente attraverso password o codici di accesso. Le significhiamo che suddetti codici non potranno essere comunicati o divulgati a terzi e ne è vietata la trascrizione su fogli. In caso di perdita o divulgazione delle credenziali d'accesso, Lei dovrà darne immediata comunicazione all'Amministratore di sistema;
- custodire con diligenza il materiale cartaceo contenente dati personali ed impedirne la visione a soggetti terzi adottando politiche di "scrivania pulita" e provvedendo, al termine dell'attività, a riporlo in appositi spazi/contenitori chiusi a chiave;
- evitare di lasciare incustodito il materiale contenente dati personali che sia salvato su supporti magnetici, digitali e informatici. È vietato trasferire il suddetto materiale al di fuori delle aree di lavoro in cui avvengono i trattamenti;
- trattare i dati personali nel rispetto dei principi di riservatezza e dignità dell'interessato;
- vigilare, insieme al Titolare del Trattamento, affinché gli interessati ricevano una adeguata informativa sul trattamento dei propri dati e, ove previsto, sia raccolto il loro consenso;
- evitare che vengano operati trattamenti (compresa la diffusione o comunicazione a terzi) senza il consenso dell'interessato ovvero senza le condizioni di liceità che ne legittimano il trattamento in assenza del suddetto consenso;
- adottare le misure richieste dall'art. 32 del Regolamento UE 2016/679 ed informare tempestivamente il Titolare qualora ravveda delle difficoltà nel porre in atto tali adempimenti;
- informare immediatamente il Titolare qualora venga a conoscenza di una violazione della sicurezza dei dati personali nonché coadiuvarlo nel garantire, in tale evenienza, il rispetto degli obblighi di cui agli artt. 33 e 34 del GDPR;
- coadiuvare il Titolare nell'evasione di richieste di esercizio dei diritti dell'interessato qualora ineriscano all'area di Sua competenza;
- informare il Titolare circa eventuali nuovi trattamenti di dati personali nell'ambito della Sua area di competenza affinché sia possibile provvedere a mettere in atto le misure necessarie per la loro tutela;

- supportare il Titolare nella gestione e manutenzione del Registro dei trattamenti per quanto concerne l'area di Sua competenza, fornendo tutte le informazioni e la documentazione necessarie a tale fine;
- adottare misure tecniche ed organizzative atte a garantire che, per impostazione predefinita, siano trattati unicamente dati necessari per le finalità perseguite nonché adeguate al fine di dimostrare che il trattamento sia stato effettuato in conformità alla normativa vigente;
- coinvolgere tempestivamente il Responsabile della Protezione dei dati in tutte le questioni attinenti alla materia della protezione dei dati personali ed altresì supportare e coadiuvare l'attività di suddetto soggetto fornendogli tutte le informazioni utili all'espletamento dei compiti affidati a tale figura;
- supervisionare l'attività degli autorizzati al trattamento dei dati che operino nella Sua area di competenza di modo che il trattamento dei dati avvenga nel rispetto della normativa vigente e delle istruzioni impartite dal Titolare del trattamento;
- individuare insieme al Titolare le aree di pertinenza di ogni autorizzato che operi nella Sua area di competenza.

COMPITI ATTINENTI ALLA GESTIONE DELLA VIDEOSORVEGLIANZA

Il Designato privacy per la videosorveglianza, nell'eseguire le attività di gestione di tale impianto, è tenuto al rispetto delle disposizioni vigenti nel settore della protezione dei dati personali, tra le quali sono da ricomprendere anche i Provvedimenti del Garante per la protezione dei dati (cfr. Provvedimento generale dell'8 aprile 2010), e della normativa concernente il controllo a distanza dei lavoratori. Egli, inoltre, si dovrà attenere a quanto disposto nel Regolamento adottato da codesto Ente in punto di gestione e manutenzione del sistema di videosorveglianza che prevede, in particolare, che il designato:

- assicurarsi che le informative brevi concernenti il trattamento dei dati mediante i sistemi di videosorveglianza siano regolarmente presenti in corrispondenza delle telecamere;
- assicurarsi che la raccolta ed il trattamento delle immagini sia limitato a quanto strettamente necessario al perseguimento delle finalità perseguite dal Titolare con l'installazione dei sistemi di videosorveglianza;
- sovrintendere l'attività dei soggetti autorizzati al trattamento dei dati derivanti dai sistemi di videosorveglianza, istruendoli sulle modalità di trattamento e vigilando sul rispetto delle istruzioni operative ricevute dagli stessi;
- sovrintendere l'attività dei responsabili esterni nominati dal Titolare nell'ambito della gestione dei sistemi di videosorveglianza;
- comunicare all'Amministratore dei sistemi di videosorveglianza l'elenco dei soggetti autorizzati al trattamento dei dati derivanti dai sistemi di videosorveglianza con specificazione del livello di accesso e l'ambito di trattamento consentito a ciascuno;
- provvedere alla tenuta del registro degli accessi alle immagini registrate;
- rispettare l'accordo sindacale/l'autorizzazione dell'Ispettorato del Lavoro nonché prevedere la comunicazione preventiva alle rappresentanze sindacali/Ispettorato del Lavoro qualora si ritenga di operare dei mutamenti ai sistemi di videosorveglianza ovvero ai presupposti legittimanti gli stessi;

-
- in caso di installazione di impianti che prevedano il ricorso a nuove tecnologie, prima di procedere al trattamento, attenzionare il Responsabile della Protezione dei Dati al fine di riceverne idoneo supporto;
 - Adottare misure necessarie affinché l'accesso ai locali e/o archivi della videosorveglianza sia protetto;
 - verificare che venga rispettato il periodo di conservazione delle immagini come disposto dal regolamento di videosorveglianza;
 - predisporre un piano di formazione nel caso di nuove assunzioni o cambio di mansioni degli Incaricati della Videosorveglianza.

Il Designato privacy dichiara di ottemperare alle istruzioni ricevute e di svolgere i compiti affidategli quali parti integrati della prestazione lavorativa dallo stesso prestata per il Titolare.

Si sottolinea che, in caso di inosservanza degli obblighi derivanti dalla presente nomina, la normativa privacy vigente prevede l'irrogazione di sanzioni civili e penali nonché provvedimenti da parte dell'Autorità Garante. Quest'ultima inoltre, qualora ravvedesse dei trattamenti illeciti o non conformi, potrà disporre ispezioni di verifica e bloccare i trattamenti in essere

Luogo, data

Titolare

Firma

Designato

Firma

f. Nomina ad Autorizzato della videosorveglianza

NOMINA AD AUTORIZZATO/A AL TRATTAMENTO DEI DATI PERSONALI CON FUZIONI DI VIDEOSORVEGLIANZA, AI SENSI DELL'ARTICOLO 29 DEL GDPR 679/2016 E AI SENSI DELL'ART. 2 QUATERDECIES DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 E SS.MM.II.).

Egr. Sig.re / Gent.le Sig.ra

CONSIDERATO

- l'incarico ricoperto dalla S.V. all'interno di questo Ente;
- quanto disposto dal Regolamento Europeo in materia di protezione dei dati personale 679/2016 (GDPR), che regola il trattamento dei dati personali;
- che per trattamento si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" (art. 4, n. 2 GDPR);

La S.V. riveste il ruolo di

AUTORIZZATO/A

La presente autorizzazione, pertanto, le consente di trattare i dati personali relativi ai seguenti trattamenti:

- *Indicare il livello di autorizzazione impartito al singolo dipendente autorizzato*

Le rammentiamo che tale ruolo impone il rispetto di quanto disposto dall'art. 5 GDPR, il quale prescrive che i dati personali oggetto del di trattamento siano:

- 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, conformemente all'articolo 89, paragrafo 1, 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 («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 («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 («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 («integrità e riservatezza»).

Le viene richiesta altresì particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli appartenenti a categorie particolari (art. 9 GDPR) e quelli relativi a condanne penali e reati, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi, nonché procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali.

MODALITÀ OPERATIVE GENERALI DA SEGUIRE PER IL TRATTAMENTO DEI DATI

Al fine della corretta gestione dei dati in trattamento Le prescriviamo le seguenti indicazioni:

- impiegare la massima cura ed attenzione nella custodia del proprio codice identificativo personale (username) e della password di accesso agli strumenti elettronici dell'Ente.
- accedere ai sistemi informatici del Titolare unicamente attraverso password o codici di accesso. Le significhiamo che suddetti codici non potranno essere comunicati o divulgati a terzi e ne è vietata la trascrizione su fogli. In caso di perdita o divulgazione delle credenziali d'accesso, Lei dovrà darne immediata comunicazione all'Amministratore di sistema;
- nel rapportarsi con soggetti terzi, accertarsi che questi siano a conoscenza del trattamento dei propri dati e, ove previsto, abbiano rilasciato il loro consenso. Ancora, qualora detti soggetti richiedano informazioni telefoniche ovvero il ritiro di documenti, Lei dovrà accertare la loro identità e la loro autorizzazione a ricevere le informazioni ed i documenti richiesti;
- trattare i dati personali nel rispetto dei principi di riservatezza e dignità dell'interessato;
- 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, alle istruzioni comunque impartite dal Titolare del Trattamento;
- evitare che vengano operati trattamenti (compresa la diffusione o comunicazione a terzi) senza

il consenso dell'interessato ovvero senza le condizioni di liceità che ne legittimano il trattamento in assenza del suddetto consenso;

- custodire con diligenza il materiale cartaceo contenente dati personali ed impedirne la visione a soggetti terzi adottando politiche di “scrivania pulita” e provvedendo, al termine dell'attività, a riporlo in appositi spazi/contenitori chiusi a chiave;
- evitare di lasciare incustodito il materiale contenente dati personali che sia salvato su supporti magnetici, digitali e informatici. È vietato trasferire il suddetto materiale al di fuori delle aree di lavoro in cui avvengono i trattamenti;
- durante l'orario di lavoro, non dovrà mai lasciare incustoditi e, o accessibili a terzi gli strumenti elettronici;
- una volta terminate le ragioni per la consultazione dei dati suddetti, procedere alla loro archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici;
- prima di lasciare il posto di lavoro, dovrà provvedere alla messa in sicurezza dei dati;
- seguire i corsi di formazione in materia di protezione dei dati personali, secondo le indicazioni e modalità date dal Titolare;
- collaborare con il Titolare, i soggetti da quest'ultimo incaricati (tra i quali il Designato privacy di riferimento) nonché con il Responsabile della Protezione dei dati segnalando eventuali criticità in merito al trattamento dei dati;
- fornire al Titolare, ai soggetti da quest'ultimo incaricati (tra i quali il Designato privacy di riferimento) nonché al Responsabile della Protezione la più ampia collaborazione, riferendo anche tutte le informazioni relative al trattamento svolto, al fine di permettere le idonee verifiche e di garantire l'aderenza alle prescrizioni previste dalla normativa vigente.

ISTRUZIONI OPERATIVE ATTINENTI ALLA GESTIONE DELLA VIDEOSORVEGLIANZA

Nell'ambito delle mansioni a Lei affidate per le attività attinenti alla gestione dei sistemi di videosorveglianza, Le vengono impartite le seguenti istruzioni atte a garantire il rispetto delle disposizioni vigenti nel settore della protezione dei dati personali:

- accedere alle immagini dei sistemi di videosorveglianza tramite le credenziali di accesso personali ed unicamente nei limiti del livello di accesso e dell'ambito di trattamento a non comunicare o divulgare a terzi e né trascrivere su fogli credenziali di accesso personali sopracitate. In caso di perdita o divulgazione delle credenziali d'accesso, Lei dovrà darne immediata comunicazione al Delegato privacy per la videosorveglianza;
- trattare i dati personali garantendo la massima riservatezza delle informazioni conosciute e, dunque, non divulgare a terzi le stesse;
- segnalare immediatamente al Designato privacy per la videosorveglianza le ragioni di cui sia eventualmente a conoscenza che giustifichino la necessità/opportunità di accedere alle immagini registrate;
- segnalare al designato della videosorveglianza eventuali reclami/ricieste da parte di Terzi, nonché qualunque fatto che a Suo giudizio possa compromettere la sicurezza delle immagini e/o la riservatezza dei dati;

- attenersi alle istruzioni e direttive impartite dal Designato privacy per la videosorveglianza nonché alle disposizioni del Regolamento di gestione dei sistemi di videosorveglianza.

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono da Lei dovuti in base al vigente contratto di lavoro. Nel caso di inadempimento si applicheranno le sanzioni disciplinari previste dal vigente contratto di lavoro e dal codice di comportamento.

La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro, per qualsiasi causa oppure fino a modifica o revoca da parte di questo Ente.

Si sottolinea che, in caso di inosservanza degli obblighi derivanti dalla presente nomina, la normativa privacy vigente prevede l'irrogazione di sanzioni civili e penali nonché provvedimenti da parte dell'Autorità Garante. Quest'ultima inoltre, qualora ravvedesse dei trattamenti illeciti o non conformi, potrà disporre ispezioni di verifica e bloccare i trattamenti in essere.

Si chiede di firmare e restituire copia del presente documento.

Luogo, data

Titolare

Firma

Autorizzato

Firma

g. Nomina a Responsabile esterno con funzioni di Amministratore di Sistema

CONTRATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N. 679 (GDPR)

TRA

..... (P. IVA), in persona del suo
Rappresentante legale pro tempore, con sede in,
(Titolare del trattamento/Titolare)

E

..... (P. IVA), in persona del suo
Rappresentante legale pro tempore, con sede in,
(Responsabile del trattamento/Responsabile)

PREMESSO CHE:

- Il titolare del trattamento di dati personali può proporre una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo quale responsabile al trattamento dei dati che sia nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo di sicurezza;
- il responsabile del trattamento deve inoltre presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa richiesti dalle disposizioni pro tempore vigenti in materia e, altresì, garantisca la tutela dei diritti dell'interessato;
- il responsabile deve procedere al trattamento secondo le istruzioni impartite dal titolare per iscritto, mediante il presente contratto e/o con eventuali accordi successivi;
- è intenzione del titolare consentire l'accesso sia al responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza è necessaria per adempiere ai compiti loro attribuiti;
- è titolare del trattamento di dati personali;
- si occupa per della gestione/manutenzione dei sistemi di videosorveglianza, ai sensi del contratto in essere tra le parti, stipulato in data, e dunque tale attività comporta la necessità per di procedere al trattamento di dati personali di utenti e dipendenti di;
- l'accesso a tali dati è limitato ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati a in base al contratto sopracitato;
- sussistono in capo a i requisiti su detti, imposti dall'art.28 GDPR.

In virtù di quanto sopra premesso, che costituisce parte integrante del presente accordo, Titolare
NOMINA

..... "Responsabile del Trattamento con funzioni di Amministratore esterno dei sistemi di videosorveglianza" ai sensi e agli effetti dell'art. 28 GDPR per i trattamenti di tutti i dati personali realizzati nell'ambito dell'incarico conferito.

In tale qualità è tenuto/a al rispetto delle disposizioni legislative vigenti nonché de provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

In particolare, è tenuto a osservare le disposizioni che seguono:

DESCRIZIONE DEL TRATTAMENTO DEL RESPONSABILE

Il Responsabile è autorizzato a trattare, per conto del Titolare del trattamento, i dati personali necessari per fornire i servizi oggetto del contratto in essere tra le parti, che costituisce il presupposto necessario del presente.

OBBLIGHI DEL RESPONSABILE IN QUALITA' DI AMMINISTRATORE DI SISTEMA

- Individuare le politiche che dovranno essere adottate per garantire la massima protezione dei sistemi contro i virus informatici e verificarne l'efficacia ogni tre mesi. Inoltre, egli dovrà assicurare e gestire adeguati sistemi di salvataggio e di ripristino dei dati (backup/recovery) anche automatici.
- Proteggere gli elaboratori dal rischio di accesso da parte di personale interno privo di autorizzazione nonché da parte di soggetti esterni.
- Garantire la sicurezza dei dati particolari e/o giudiziari contro l'accesso da parte di chiunque abusivamente si introduca nel sistema informatico o telematico.
- Predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte sua (nella sua qualità di amministratore di sistema); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- Adottare le misure di sicurezza in base all'art. 32 del Regolamento UE 2016/679 come meglio precisato nell'allegato.
- Dare tempestiva comunicazione al Titolare del trattamento dei dati personali qualora vengano rilevati rischi relativamente alle misure di sicurezza predisposte per la protezione dei dati tratta
- Coordinare, assieme al Titolare, le attività operative degli autorizzati al trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento delle informazioni nell'ambito del sistema informatico.
- Collaborare con il Titolare per l'attuazione delle prescrizioni impartite dal Garante.
- Trattare i dati personali unicamente su istruzione documentata del Titolare e nel rispetto dell'obbligo di riservatezza;
- Non utilizzare i dati trattati e le informazioni acquisite per finalità diverse da quelle immanenti all'oggetto del contratto sottoscritto.
- Adottare misure tecniche ed organizzative atte a garantire e dimostrare che il trattamento sia effettuato in conformità alla normativa vigente;
- Mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art.28 del Regolamento UE 2016/679, consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.
- Assistere il Titolare nella predisposizione di misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
- Individuare, all'interno della propria organizzazione, i soggetti muniti dei necessari requisiti

di esperienza, capacità e affidabilità cui demandare le mansioni oggetto del contratto sottoscritto nonché delimitarne gli ambiti di operatività.

- Garantire che le persone autorizzate al trattamento dei dati personali siano impegnate alla riservatezza ed altresì che le stesse ricevano idonee istruzioni scritte concernenti le modalità per lo svolgimento delle operazioni di trattamento.
- Mettere a disposizione del Titolare l'elenco aggiornato dei nominativi delle persone che saranno assegnate a questo Ente per l'espletamento del Vostro incarico e comunicare tempestivamente eventuali le modifiche nell'assegnazione.
- Impegnarsi ad un controllo periodico sull'operato dei soggetti autorizzati ed altresì gestire sistemi idonei di registrazione degli accessi logici ai sistemi di videosorveglianza da parte dei sopracitati soggetti.
- Assistere il Titolare con misure tecniche ed organizzative adeguate, nella misura di quanto possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste di esercizio dei diritti da parte degli interessati ai sensi del Regolamento UE 2016/679.
- Tenere il registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento ai sensi dell'art. 30 par. 2 del Regolamento UE 2016/679.
- In base a quanto previsto all'allegato, assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza, di notifica della violazione dei dati ed in materia di valutazione d'impatto nonché informarlo, senza ingiustificato ritardo, delle violazioni dei dati o degli incidenti informatici che possono avere un impatto significativo sui dati personali trattati.

OBBLIGHI SPECIFICI IN RELAZIONE ALLA VIDEOSORVEGLIANZA

Il Responsabile, nell'eseguire le mansioni affidategli in relazione ai sistemi di videosorveglianza è tenuto all'osservanza dei seguenti obblighi:

- Trattare le immagini esclusivamente allo scopo di consentire al Titolare di perseguire le finalità di cui all'Informativa privacy in materia di videosorveglianza.
- Garantire le funzionalità dei sistemi di videosorveglianza come stabilite nell'accordo contrattuale siglato mantenendo, ove previsto, le immagini registrate in formato elettronico nel N.V.R. per il periodo definito nel Regolamento adottato da codesto Ente con riferimento alla videosorveglianza, periodo oltre il quale le immagini verranno cancellate mediante sovrascrittura.
- Prevedere l'ulteriore conservazione delle immagini registrate per i periodi festivi nonché nei casi previsti nel Regolamento di Videosorveglianza dell'Ente;
- Generare le credenziali di accesso per il personale dell'Ente specificamente autorizzato consentendo a ciascuno di operare unicamente nei limiti del livello di accesso e dell'ambito di trattamento consentitogli dal Titolare;
- Consentire al personale del titolare, appositamente nominato, di richiedere modifiche unicamente sulla base di una specifica richiesta scritta del titolare e istituire il relativo registro;
- Attribuire al personale adibito alla semplice manutenzione dei sistemi di videosorveglianza credenziali che non permettano la visione delle immagini;
- Istituire un registro degli interventi di manutenzione all'impianto di videosorveglianza in cui sia riportata la data e l'ora dell'intervento nonché l'identità del soggetto incaricato;
- Garantire il rispetto del Regolamento aziendale approvato da codesto Ente.

NOMINA DI ULTERIORE RESPONSABILE ESTERNO DEL TRATTAMENTO (O SUB RESPONSABILE)

Il Titolare del trattamento deve autorizzare a sub-delegare ad altro Responsabile trattamenti di dati demandati in forza del contratto tra le parti.

A tale autorizzazione segue l'atto di nomina del sub-responsabile che deve essere inoltrato dal Responsabile al Titolare.

Parimenti, il Responsabile informa il Titolare anche di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili, così da permettergli di esercitare il diritto di opporsi.

Spetta in capo al Responsabile del trattamento l'obbligo di assicurarsi che il sub-responsabile presenti le garanzie sufficienti per quanto riguarda l'adozione delle misure tecniche e organizzative necessarie affinché il trattamento dei dati sia conforme alle esigenze del GDPR. Se il sub-responsabile non rispetta gli obblighi in materia di protezione dei dati personali, il Responsabile risponde solidalmente nei confronti del Titolare del trattamento.

VERIFICHE PERIODICHE/ AUDIT

Il Responsabile esterno deve fornire la massima disponibilità e collaborazione, consentendo, se necessario, l'accesso ai propri locali, nonché la verifica delle procedure applicate nella gestione dei documenti cartacei ed elettronici affinché il Titolare possa svolgere, anche tramite consulenti ed addetti di propria fiducia, le "verifiche periodiche" previste dall'art. 28 GDPR, necessarie per accertarsi del rispetto degli obblighi di questo accordo e della normativa sopra citata.

Il Responsabile riferisce per iscritto al Titolare, sui dettagli relativi all'adempimento di quanto disposto dalla Legge e dal presente atto di nomina, ogni qualvolta quest'ultimo ne faccia richiesta.

GESTIONE MODULISTICA PRIVACY

Il Responsabile esterno deve operare in maniera conforme ai principi di efficienza e trasparenza, tramite adeguate procedure e garantendo la custodia, la non alterazione e l'agevole reperimento della documentazione relativa agli adempimenti formali prescritti dalla normativa.

Il Responsabile esterno, su richiesta del Titolare, deve coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi al Garante per la protezione dei dati personali o all'Autorità giudiziaria ordinaria anche consentendogli la tempestiva esibizione della modulistica privacy e dei documenti probatori rientranti nella competenza del Responsabile stesso.

CESSAZIONE DEL RAPPORTO

All'atto della cessazione, per qualsiasi causa intervenuta, delle operazioni di trattamento da parte del Responsabile, quest'ultimo, su scelta del Titolare, cancella o restituisce tempestivamente – e comunque entro un mese - i dati personali oggetto delle operazioni di trattamento, su qualunque supporto detenuto (cartaceo o informatico, originali e copie), provvedendo altresì a cancellarne eventuali copie esistenti e rilasciando un'attestazione scritta di tali circostanze. Ciò salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati.

DURATA

La presente nomina avrà durata pari a quella del contratto principale in essere tra le parti e cesserà di diritto alla cessazione, per qualsiasi causa occorsa, dello stesso.

REVOCA

Il Titolare ha facoltà di revocare il presente mandato nel caso di reiterate violazioni GDPR con effetto immediato, previa notifica scritta allo stesso via PEC e senza che nulla sia ulteriormente dovuto.

LEGGE APPLICABILE E FORO COMPETENTE

Il presente contratto è disciplinato secondo la Legge Italiana. Per quanto ivi non esplicitamente previsto si applicheranno le norme del Codice Civile nonché le altre norme giuridiche inderogabili aventi efficacia di legge.

Si sottolinea che, in caso di inosservanza degli obblighi derivanti dalla presente nomina, la normativa

privacy vigente prevede l'irrogazione di sanzioni civili e penali nonché provvedimenti da parte dell'Autorità Garante. Quest'ultima inoltre, qualora ravvedesse dei trattamenti illeciti o non conformi, potrà disporre ispezioni di verifica e bloccare i trattamenti in essere

Tutte le controversie derivanti dal presente contratto, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, saranno di competenza esclusiva del Foro già individuato nel contratto principale.

Luogo, Data

Titolare del trattamento

Firma

Responsabile

Firma

ALLEGATO - MISURE DI SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei 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.

A tale scopo dovrà assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi utilizzati per lo svolgimento delle attività di cui al contratto.

In caso si difficoltà nell'adozione delle sopracitate misure, il Responsabile dovrà tempestivamente informare il Titolare e farsi parte attiva nell'individuazione e predisposizione della soluzione più adeguate al caso di specie.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Il Responsabile del trattamento, se necessario e su richiesta, dovrà altresì assistere il Titolare del trattamento nella redazione del "DPIA" (Data Protection Impact Assessment), contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere in merito un parere al DPO (Data Protection Officer) (art.35 e C.90 GDPR).

Violazione dei dati. Se dovesse venire a conoscenza di una violazione dei dati personali (Data Breach), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).

Il Responsabile deve coadiuvare il Titolare del trattamento nella redazione di specifiche procedure che consentono di individuare prontamente le violazioni dei dati subite (Data Breach) e le relative procedure di risposta attraverso l'elaborazione di una specifica policy.

La suddetta policy deve includere, tra le altre cose:

- le linee guida per valutare le violazioni di dati subite al fine di individuare quelle che sono suscettibili di presentare un elevato rischio per i diritti e le libertà delle persone fisiche e che dunque dovranno essere notificate all'Autorità di controllo competente;
- le linee guida sulla scelta delle informazioni che saranno rese disponibili all'interessato dal Titolare del trattamento attraverso la comunicazione della violazione, se dalla valutazione precedentemente effettuata, fosse risultata suscettibile di presentare rischi elevati per i diritti e le libertà dell'interessato.

Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

Nello specifico dovranno essere documentati:

- a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) il nome e i dati di contatto de DPO (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
- c) la descrizione delle probabili conseguenze della violazione dei dati personali;
- d) le descrizioni delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (Data breach) prevista dall'art. 33 comma 3 del GDPR.

h. Informativa personale dipendente

A TUTTI I DIPENDENTI

Oggetto: INFORMATIVA AI DIPENDENTI – VIDEOSORVEGLIANZA - attivazione, posizionamento e modalità di funzionamento

Il legale rappresentante dell'Ente....., con sede legale in

PREMESSO CHE

- nelle attività di videosorveglianza è necessario rispettare l'art. 4 dello Statuto dei Lavoratori (Legge n. 300/1970) e, dunque, è vietato operare il controllo a distanza dell'attività lavorativa.
- Inoltre, in base a tale disciplina normativa, devono essere osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro.
- Tali garanzie devono essere rispettate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro.
- È inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi).

INFORMA CHE

- L'Ente utilizza un sistema di videosorveglianza interna ed esterna al solo fine di garantire: La tutela del patrimonio dell'Ente da possibili furti, rapine, danneggiamenti, atti di vandalici o eventi simili; la sicurezza e l'incolumità dei lavoratori e dei visitatori all'interno delle strutture; implementazione dei sistemi di incolumità e assistenza degli ospiti del Nucleo Alzheimer;
- Sono presenti apparecchiature di videosorveglianza h24;
- Che sono presenti apparecchiature di videocontrollo nella guardiola del nucleo Alzheimer in funzione h24.
- Le immagini sono registrate e conservate esclusivamente a cura del personale addetto e sono cancellate entro 168 ore dalla rilevazione, salvo eventuali periodi legati a festività o chiusura, nel rispetto del punto 3.4 del provvedimento del Garante per la protezione dei dati personali del 8.4.2010 e della normativa vigente. Le immagini sono consultabili solo dal personale autorizzato o dall'autorità giudiziaria o di polizia.
- L'impianto e le apparecchiature non riprenderanno luoghi riservati esclusivamente ai dipendenti.
- L'impianto registrerà solo le immagini indispensabili ed è costituito da telecamere orientate verso le aree (limitando l'angolo delle riprese ed evitando, quando non indispensabili, immagini dettagliate).
- L'eventuale ripresa di dipendenti avverrà esclusivamente in via incidentale e con criteri di occasionalità.
- All'impianto non potrà essere apportata alcuna modifica e non potrà essere aggiunta alcuna ulteriore apparecchiatura (se non in conformità all'art. 4 della Legge n. 300/1970 e sempre previa relativa autorizzazione della D.T.L. o accordo con le rappresentanze sindacali).

- Il trattamento dei dati personali avverrà nel rispetto dei diritti e delle libertà fondamentali dei cittadini e della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali.
- Le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro.
- I lavoratori potranno verificare periodicamente il corretto utilizzo dell'impianto.

In osservanza di quanto previsto dalle disposizioni di legge La informiamo, come sopra, circa le finalità e le modalità delle immagini registrate.

In particolare:

- Finalità: La tutela del patrimonio dell'Ente da possibili furti, rapine, danneggiamenti, atti di vandalici o eventi simili; la sicurezza e l'incolumità dei lavoratori e dei visitatori all'interno delle strutture; implementazione dei sistemi di incolumità e assistenza degli ospiti del Nucleo Alzheimer;
- Base giuridica: La base giuridica del trattamento è data dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'art. 6, parag. 1, lett. e, del Regolamento UE 2016/679 e dalla necessità di adempiere un obbligo legale al quale è soggetto il titolare del trattamento ai sensi dell'art. 6, parag. 1, lett. c, del Regolamento UE 2016/679 (DGR 84/2007).
- Modalità e durata della conservazione: il trattamento dei dati è eseguito attraverso procedure informatiche e la eventuale visualizzazione avviene solo ad opera di soggetti autorizzati nonché da parte del Responsabile esterno del trattamento che si occupa di manutenzione/gestione dei sistemi di videosorveglianza. I dati vengono conservati per la durata massima di 168 con successiva cancellazione automatica.

Per ulteriori informazioni in merito al trattamento dei dati si rinvia all'informativa estesa allegata.

_____ il _____

Il Legale Rappresentante