

Allegato 5



DISCIPLINARE PER I TRATTAMENTI RELATIVI ALLA VIDEOSORVEGLIANZA

ai sensi del Regolamento UE 679/2016, delle linee guida n. 3/2019 dell'EDPB e delle indicazioni del Garante

1 - PREMESSA

1.1. – OBIETTIVI E CAMPO DI APPLICAZIONE

Premesse alcune indicazioni generali sulla disciplina della videosorveglianza, obiettivi del presente documento sono quelli di descrivere i principi, le regole e le procedure di:

- A. gestione del servizio di videosorveglianza presso le aree di pertinenza della Camera di commercio di Reggio Calabria (di seguito anche “Camera di commercio” o “Titolare” o “Ente”), ubicati nei locali della sede camerale in via Tommaso Campanella n. 12, considerati come siti soggetti a rischi;
- B. trattamento, quali ad es., l’accesso alle immagini registrate e la realizzazione di copie di sicurezza, la loro conservazione e la consegna su richiesta, ad uso esclusivo delle Autorità (Magistratura e Forze dell’Ordine o altri soggetti, secondo le previsioni di legge)¹.

La procedura è di tipo organizzativo. Il suo fine è quello di:

1. individuare i soggetti autorizzati, evidenziandone ruoli, attività, compiti e responsabilità;
2. enunciare le direttive per una gestione delle immagini ed in particolare delle registrazioni in conformità con la legge vigente, tenuto conto delle esigenze concrete per cui il trattamento viene effettuato.

La procedura di cui al presente Disciplinare non riguarda la videosorveglianza dei lavoratori che – se prevista - è soggetta ad una disciplina specifica, alla quale si rinvia².

1.2. - RIFERIMENTI NORMATIVI PRINCIPALI

Il presente documento risponde ai seguenti requisiti normativi:

1. Titolare del trattamento (art. 4, n. 7 e art. 24 del GDPR);
2. Responsabile della Protezione dei Dati (art. 37, 38 e 39 del GDPR);
3. Responsabile esterno del trattamento dei dati (art. 28 del GDPR);
4. Soggetti che trattano dati “per conto” e sotto l’autorità del Titolare del trattamento (art. 29 del GDPR);

¹ Le “Forze dell’ordine” sono costituite dai corpi militari e civili dello Stato o degli enti pubblici territoriali, competenti alla tutela dell’ordine, della sicurezza pubblica e, se necessario, dei servizi di pubblico soccorso. L’art. 16 della legge n. 121/1981 comprende: la Polizia di Stato, l’Arma dei Carabinieri, la Guardia di finanza, nonché la Polizia penitenziaria e il Corpo forestale dello Stato (quest’ultimo, nel 2016, è stato sciolto ed il personale assegnato ad altre forze di polizia, in prevalenza nell’Arma dei carabinieri).

Fanno parte delle forze dell’ordine anche la Guardia costiera, che dipende dal Ministero delle Infrastrutture e dei Trasporti con ordinamento militare all’interno della Marina militare, nonché la polizia locale (detta anche “municipale”), di cui alla legge n. 65/1986 e successive leggi regionali specifiche.

Si tenga inoltre presente il concetto di “Autorità competente” previsto dal D.Lgs. 18 maggio 2018, n. 51 (*Attuazione della direttiva (UE) 2016/680 del parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*). L’art. 2, comma 1, lett. g), prevede che l’“autorità competente” è “1) qualsiasi autorità pubblica dello Stato, di uno Stato membro dell’Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; 2) qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l’autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica”.

² La frase è prevista per mera completezza dell’esposizione, posto che nella maggioranza dei casi le Camere di commercio non prevedono la videosorveglianza dei lavoratori.

5. Artt. 32-36 del GDPR (sicurezza dei trattamenti e valutazione di impatto);
6. Attribuzione di funzioni e compiti a soggetti designati (art. 2-*quaterdecies* del D.Lgs. n. 196/2003);
7. EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video (Versione 2.0), adottate il 29 gennaio 2020, in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it;
8. Garante per la protezione dei dati personali, Provv. 8 aprile 2010, in materia di Videosorveglianza;
9. Garante, *FAQ in tema di videosorveglianza*, in <https://www.garanteprivacy.it/temi/videosorveglianza>.

1.3. - ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE n. 679/2016 (General Data Protection Regulation)
Codice	D.Lgs. n. 196/2003 “Codice in materia di protezione dei dati personali”
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo per la protezione dei dati - EDPB)
EDPB	European Data Protection Board v. WP29
RPD/DPO	Responsabile della Protezione dei Dati/ <i>Data Protection Officer</i>
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della <i>compliance</i> al GDPR
SG	Segretario Generale della Camera di commercio di _____
AdS	Amministratore di Sistema nominato sulla base delle Linee guida della Camera di commercio, adottate ai sensi del GDPR e del Provv. del Garante del 27 novembre 2008

1.4. - ULTERIORI INDICAZIONI E RINVIO AD ALTRI DOCUMENTI

Il Disciplinare e le prescrizioni definite al suo interno, con specifico riferimento alle Parti da II a V (compresi i relativi allegati):

- a) deve essere conosciuto e condiviso, ognuno per la propria Area/Servizio/Ufficio e per le mansioni di competenza. A questo riguardo sarà oggetto di una specifica attività di divulgazione/formazione;
- b) devono intendersi quali istruzioni impartite dal Titolare, il cui mancato rispetto costituisce inosservanza delle disposizioni al personale;
- c) integrano e completano, reciprocamente, le indicazioni contenute:
 - nel “Disciplinare tecnico per l’utilizzo degli strumenti informatici, telematici e principali misure di sicurezza”;
 - nelle “Linee guida per la realizzazione di una valutazione di impatto del trattamento di dati (DPIA)”.

2 - PARTE I – CENNI GENERALI SULLA DISCIPLINA DELLA VIDEOSORVEGLIANZA

2.1. – IL PROVVEDIMENTO DEL GARANTE E LE LINEE GUIDA DELL'EDPB

In via preliminare va fatto presente che, nel nostro ordinamento, non è presente una definizione che individui specificamente cosa si debba intendere per “videosorveglianza”, né si rinviene una disciplina organica in materia. Il tema, infatti, è affrontato nell’ambito di norme specifiche, tra le quali – per i rispettivi ambiti – le disposizioni penali sul divieto di interferenze nella vita privata, la tutela del domicilio; le disposizioni del codice civile (e della legge sul diritto di autore), sulla tutela dell’immagine; lo statuto dei lavoratori, sul divieto di “monitoraggio”, etc.

Il WP 29, nel parere n. 4/2004 (documento WP89), ha definito la videosorveglianza come l’“attività mirante al controllo a distanza di eventi, situazioni e avvenimenti” mediante l’“acquisizione di immagini, eventualmente in associazione con dati sonori e/o biometrici”. Con riferimento ai ‘componenti’ di un sistema di videosorveglianza possiamo indicare i seguenti: a) mezzi di ripresa; b) mezzi di visualizzazione; c) mezzi di registrazione/archiviazione; d) mezzi di trasmissione/comunicazione. In tutti gli ambiti indicati trovano applicazione i principi del GDPR.

Il Garante, data la rilevanza dell’argomento³, ha dettato una regolazione con il Provv. 29 aprile 2004, poi sostituito con il Provv. 8 aprile 2010⁴. Questo provvedimento – nella sua natura prescrittiva (essendo stato emanato ai sensi dell’art. 154, comma 1, lett., c), del Codice privacy)⁵ – non è stato abrogato dal GDPR ed è ancora in vigore, ai sensi dell’art. 22, comma 4, del D.Lgs. n. 101/2018, secondo il quale “a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto”.

Sulla videosorveglianza, il Comitato europeo per la protezione dei dati (EDPB – European Data Protection Board) ha predisposto delle «Linee guida sul trattamento dei dati personali attraverso dispositivi video», definitivamente adottate, nella versione 2.0., il 29 gennaio 2020.

Conseguentemente, i contenuti del citato Provvedimento del Garante devono essere letti tenuto conto delle intervenute disposizioni sia del GDPR che delle Linee guida dell’EDPB.

Nel prosieguo, anche in forma tabellare, saranno effettuati i confronti tra le indicazioni del Garante e quelle del Comitato (indicato anche come EDPB).

2.2. – AMBITO DI APPLICAZIONE DELLA DISCIPLINA

La disciplina sulla videosorveglianza, dal punto di vista del trattamento dei dati personali, trova applicazione nel caso di riprese di immagini di persone fisiche identificate o identificabili.

³ Secondo il Garante, «la raccolta, la registrazione, la conservazione e, in generale, l’utilizzo di immagini configura un trattamento di dati personali qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione)» nonché vi è la necessità di garantire, in particolare, un «livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, perché potenzialmente in grado di determinare un’ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati».

⁴ Pubblicato nella G.U. n. 99 del 29 aprile 2010.

⁵ Nel nuovo quadro di riferimento normativo, le Autorità di controllo non sono più dotate di poteri di regolazione generale.

L’art. 54 del GDPR prevede solo il potere di «indirizzo generale» attraverso linee guida, mentre il Codice privacy prevede: 1. l’emanazione di provvedimenti prescrittivi solo in circoscritte materie (trattamenti svolti per l’esecuzione di un compito di interesse pubblico che possono presentare rischi elevati; trattamenti a fini di ricerca scientifica o statistici); 2. la sanzionabilità delle violazioni solo di alcune tipologie di provvedimenti (es., autorizzazioni generali, provvedimento che definisce le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute).

Le Linee guida dell'EDPB indicano tre esempi tipici di non applicazione:

- 1) Il GDPR non è applicabile alle fotocamere false (vale a dire qualsiasi fotocamera che non funziona come una fotocamera e quindi non elabora alcun dato personale). *Tuttavia, in alcuni Stati membri potrebbero essere applicabili altre normative.*
- 2) Le registrazioni ad alta quota rientrano nell'ambito di applicazione del GDPR solo se, in queste circostanze, i dati trattati possono essere correlati a una determinata persona.
- 3) Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a una persona fisica (ad esempio targhe o informazioni che potrebbero identificare i passanti), il GDPR non è applicabile.

Vengono ricordate anche due situazioni generali in cui non trovano applicazione le disposizioni del GDPR:

- a) Trattamento di dati personali effettuato da una persona fisica nell'esercizio di un'attività *esclusivamente* personale o domestica;
- b) Trattamento di dati personali eseguito da parte delle autorità competenti per i fini di prevenzione, indagine, accertamento o perseguimento di reati, ovvero per l'esecuzione di sanzioni penali.

Riguardo la prima situazione, secondo quanto previsto dall'art. 2, par. 2, lett. c), del GDPR, esula dall'ambito di applicazione il trattamento per motivi personali (comprese anche le attività *online*). Tuttavia, con riferimento alla videosorveglianza, detta deroga applicativa deve essere interpretata in modo restrittivo. Come stabilito dalla Corte di giustizia, la cosiddetta «deroga relativa alle attività a carattere domestico» deve «[...] interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone»⁶.

Inoltre, un sistema di videosorveglianza, nella misura in cui comporta la registrazione e la conservazione costanti di dati personali e si estende «anche se solo parzialmente, allo spazio pubblico, e pertanto è dirett[o] verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, [...] non può essere considerat[o] un'attività esclusivamente "personale o domestica" ai sensi dell'articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46»⁷.

Riguardo la seconda situazione, si rientra nel campo di applicazione della Direttiva 2018/680/UE, attuata in Italia con il D.Lgs. 18 maggio 2018, n. 51.

2.3. – FINALITA' DELLA VIDEOSORVEGLIANZA

Prov. Garante	Linee guida EDPB
1) protezione e incolumità degli individui	1) protezione della vita e dell'integrità fisica delle persone
2) protezione della proprietà	2) protezione della proprietà e di altri beni

⁶ Corte giust. UE, sent. 6 novembre 2003, nella causa C-101/01, *Bodil Lindqvist*, punto 47.

⁷ Corte giust. UE, sent. 11 dicembre 2014, nella causa C-212/13, *František Ryneš contro Úřad pro ochranu osobních údajů*, punto 33.

3) sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge	
4) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge	
5) acquisizione di prove	3) raccolta di elementi di prova in vista di procedimenti giudiziari civili
	Le finalità del monitoraggio devono essere documentate per iscritto (articolo 5, par. 2) e devono essere specificate per ogni telecamera di sorveglianza in uso (<u>le telecamere utilizzate per lo stesso scopo da un unico titolare del trattamento possono essere oggetto di una documentazione unitaria</u>)

Si faccia attenzione che l'adozione della videosorveglianza – in specie negli ambienti di lavoro (al di là delle specifiche questioni relative, non affrontate, come detto, in questo Disciplinare) – non può avere quale finalità la prevenzione di possibili reati.

Nel 2020, il Commissario statale per la protezione dei dati (LfD) della Bassa Sassonia, ha sanzionato per 10,4 milioni di euro una società che monitorava i propri dipendenti per finalità di prevenzione dei furti. Secondo tale Autorità per tali finalità i Titolari *non possono ricorrere ad una preventiva videosorveglianza indiscriminata negli ambienti di lavoro*, ma in presenza di un sospetto devono agire gradualmente con controlli inizialmente meno invasivi, ad es. mediante controlli a campione sui bagagli di chi esce dai locali commerciali.

L'Autorità norvegese per la protezione dei dati (Datatilsynet) ha sanzionato per 37.400 euro l'Amministrazione norvegese per le strade pubbliche per aver raccolto, attraverso videocamere, immagini dei dipendenti con lo scopo di sicurezza e prevenzione degli incidenti sul lavoro. Detta Amministrazione, nonostante avesse indicato una *data retention* di 7 giorni, conservava le immagini per molti mesi al fine di documentare le violazioni dei protocolli di sicurezza nei casi di incidenti (e, quindi, l'inadempimento contrattuale). L'Autorità di controllo ha dichiarato l'illegittimità di questa finalità in quanto incompatibile con lo scopo originario che era quello di rendere possibili misure di sicurezza immediate. L'ulteriore utilizzo delle immagini perseguiva, quindi, in maniera del tutto proporzionata per i lavoratori una diversa finalità che – tra l'altro – non era stata indicata, né risultava prevedibile per gli interessati.

2.4. – BASE GIURIDICA

Affrontare il tema della base giuridica del trattamento dei dati, anche nella videosorveglianza, implica una riflessione sulle possibilità individuate nell'art. 6 del GDPR.

Provv. Garante	Linee guida EDPB
----------------	------------------

Il trattamento dei dati attraverso sistemi di videosorveglianza deve essere fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici:

- **trattamento consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2, del Codice previgente)**
- nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice previgente))
- il trattamento di dati diversi da quelli sensibili e giudiziari è consentito... anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente (art. 19, comma 1, del Codice previgente)

In linea di principio, ogni fondamento di diritto ai sensi dell'articolo 6, par. 1, può fornire una base giuridica per il trattamento dei dati della videosorveglianza.

Ad esempio, **l'articolo 6, par. 1, lett. c), si applica quando la normativa nazionale prevede l'obbligo di mettere in atto un sistema di videosorveglianza.**

Tuttavia, nella pratica, le disposizioni più suscettibili di essere utilizzate sono:

- art. 6, par. 1, lett. f): **legittimo interesse**
- art. 6, par. 1, lett. e): **necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri**

La base giuridica inerente "l'obbligo di legge" (art. 6, par 1., lett. c), del GDPR) deve essere interpretato in termini assolutamente restrittivi, nel senso che la disciplina legislativa (nazionale o europea) deve imporre l'adozione della videosorveglianza. Conseguentemente, la tutela dei beni e del patrimonio, e/o delle persone (anche in relazione alla sicurezza delle medesime ex D.Lgs. 81/2008), non può costituire una valida base giuridica, ai sensi del citato art. 6, par. 1, lett. c), posto che, al momento, non vi è un «obbligo» di installare telecamere.

Nelle indicazioni contenute nel Provvedimento del Garante si indicano specifiche ipotesi nelle quali – come previsto da norme di legge – sono indicati precisi obblighi di legge, in correlazione con lo svolgimento di attività rientranti nelle finalità istituzionali degli enti pubblici.

Gli esempi del Garante, infatti, fanno riferimento solo a trattamenti «istituzionali» costituenti e "fondanti" la *mission* di un Ente pubblico, *quindi previsti da disposizioni legislative*:

- sicurezza urbana di competenza del Sindaco e dei Comuni (ordine e sicurezza pubblica, polizia giudiziaria, polizia locale, etc.);
- deposito dei rifiuti, di competenza degli Enti locali (utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose; rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti ove sanzionabili);
- rilevazione di violazioni al Codice della strada (anche qui: polizia locale e forze di polizia in generale);
- rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, di competenza del Sindaco e dei Comuni;
- controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (qui non serve una disposizione legislativa specifica, visto che si tratta di prestazioni sanitarie necessarie);
- sicurezza nel trasporto pubblico (sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi), anche qui di competenza degli Enti locali.

⁹ Per esempio, il monitoraggio degli atleti per analizzarne tecniche e prestazioni.

Il GDPR stabilisce chiaramente che le autorità pubbliche non possono invocare il legittimo interesse per i trattamenti svolti nell'esecuzione dei loro compiti

f) perseguimento del legittimo interesse del titolare del trattamento o di terzi

Sarebbe comunque necessaria una valutazione sulla consistenza del legittimo interesse, con documentazione ad es., di eventi lesivi su beni/persone ed una specifica valutazione - «bilanciamento di interessi» - sulla prevalenza dell'interesse vantato dal titolare rispetto ai diritti e le libertà fondamentali dell'interessato¹⁰

In assenza di una base giuridica derivante dall'obbligo di legge, ovvero dallo svolgimento dei compiti istituzionali, secondo quanto chiarito in precedenza, resta percorribile la strada del ricorso al "legittimo interesse", di cui all'art. 6, par. 1, lett. f), del GDPR.

Se è vero che il GDPR stabilisce che le autorità pubbliche non possono invocare il legittimo interesse è anche vero che questa preclusione concerne unicamente "i trattamenti svolti nell'esecuzione dei loro compiti", cioè per quelle che sono le loro funzioni istituzionali, sulla base del rispetto del principio di legalità. Ciò significa che **il divieto di utilizzo dell'interesse legittimo non opererebbe nei confronti di una PA che agisce «iure privatorum»** (l'art. 1, comma 1 bis, della L. 241/1990, stabilisce che la PA nell'adozione di atti di natura non autoritativa, agisce secondo le norme di diritto privato) ad es., in relazione alla protezione dei beni e del patrimonio. E' quindi difficile sostenere che, per la difesa del suo patrimonio, un Ente pubblico agisca in una veste totalmente diversa da quella di un qualsiasi privato.

Va notato che l'EDPB non fa alcun riferimento alle basi giuridiche di cui all'art. 9 (per i dati particolari) e 10 (per i dati relativi a condanne penali e reati) del GDPR, nonostante i «sistemi di videosorveglianza (...) possono rivelare dati di natura altamente personale e persino categorie particolari di dati», questi non sempre configurano un trattamento di dati particolari. Ciò perché il trattamento di questi dati personali richiede una specifica base giuridica *unicamente nelle ipotesi in cui il sistema di videosorveglianza sia stato predisposto effettivamente (e non solo incidentalmente) per la raccolta di tali dati particolari*.

Al riguardo, l'EDPB porta come esempi, i seguenti:

- ripresa di immagini di persone che partecipano ad una manifestazione politica o sindacale;
- ripresa di immagini di pazienti in terapia intensiva.

Nelle due ipotesi, la base giuridica ravvisabile è, rispettivamente: l'art. 9, par. 2, lett. e), del GDPR (il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato) e art. 9, par. 2, lett. g), del GDPR (il trattamento è necessario per motivi di interesse pubblico rilevante).

2.5. – L'INFORMATIVA

Per la videosorveglianza – come per tutti i trattamenti – va osservato il principio di trasparenza, soprattutto perché le riprese costituiscono, con tutta evidenza, una "intromissione" nella vita personale degli interessati.

Sul tema, data la sua specificità, l'EDPB - nelle Linee guida in materia di trasparenza del 2018 – ha previsto due livelli, crescenti, di informativa.

¹⁰ I Titolari del trattamento dovrebbero documentare gli eventi problematici in questione (data, modalità, perdita finanziaria) e le relative accuse penali, etc. Le situazioni di pericolo imminente possono configurare un legittimo interesse, ad es. nel caso di banche o negozi che vendono beni preziosi (ad esempio, gioiellerie) o di luoghi che sono notoriamente teatro di reati contro il patrimonio (ad esempio, stazioni di servizio).

L'informativa di "primo livello" è costituita da un "avvertimento", ossia in un segnale (anche grazie all'uso di una icona grafica), chiaramente visibile dall'interessato che serve a renderlo edotto del trattamento se varcato lo spazio soggetto alle riprese.

Detta informativa comprende, inoltre, i dati essenziali per la tutela dell'interessato, nonché il "rinvio" su come e dove reperire l'informativa completa (che può anche essere compresa in un QR Code posto in questo primo livello di informativa).

L'informativa di "secondo livello" contiene, in dettaglio, quanto disposto dall'art. 13 del GDPR, con particolare attenzione a quelli che possono costituire espressione di maggiore presidio tutelare per l'interessato. Ad esempio, appare utile indicare se vi sia (e chi è) un Responsabile del trattamento o se vi sono comunicazioni o trasferimenti all'estero di dati personali. Indicare anche la natura – pubblica o privata – del Titolare non è privo di valore.

Di seguito un quadro delle indicazioni del Garante e dell'EDPB che si completano vicendevolmente, con riferimento all'informativa di primo livello.

Prov. Garante	Linee guida EDPB
Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata. A tal fine, era proposto un modello semplificato di informativa "minima", indicante il Titolare del trattamento e la finalità perseguita che: • deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze ¹¹; • deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale; • può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.	Il principio generale di trasparenza potrebbe estrinsecarsi in: una «informazione di primo livello» (segnaletica di avvertimento) ad es., un'icona accompagnata da un set di informazioni (per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto) quali: • le finalità del trattamento¹²; • l'identità del Titolare del trattamento; • i recapiti del Responsabile della protezione dei dati; • l'esistenza dei diritti dell'interessato. Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero <u>risultare inaspettate</u> per l'interessato (ad es., trasmissione di dati a terzi, fuori UE...). Occorre infine fare riferimento <u>alle informazioni di secondo livello</u>, più dettagliate, indicando dove e come trovarle. Le informazioni dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi).

¹¹ In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, dovranno essere installati più cartelli.

¹² Gli interessati devono essere informati delle finalità del trattamento ai sensi dell'art. 13 GDPR. La semplice menzione di uno scopo di «sicurezza» o «per la vostra sicurezza» con riguardo alla videosorveglianza non è sufficientemente specifica (art. 5, par. 1, lett. b).

Di seguito, il parallelo delle indicazioni riferite all'informativa di secondo livello.

Prov. Garante	Linee guida EDPB
Il Garante riteneva <u>auspicabile</u> che l'informativa semplificata rinviasse a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice previgente, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici, ad es. in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito	Le informazioni di secondo livello: • devono contenere tutti gli elementi obbligatori a norma dell'articolo 13 del GDPR; • devono essere facilmente accessibili per l'interessato, ad es., attraverso una pagina informativa completa messa a disposizione in uno snodo centrale (sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso. Dovrebbe essere possibile accedere al secondo livello di informazioni senza entrare nell'area videosorvegliata, ad es. tramite l'indicazione nell'informazione di primo livello: • di un link o QR code • di un numero telefonico da contattare

2.6. – ADEMPIMENTI GESTIONALI

2.6.1. – A) Autorizzazioni al trattamento

Sulle autorizzazioni al trattamento, il Garante ha sottolineato l'attenzione sui seguenti adempimenti:

- a) designare per iscritto tutte le persone fisiche, incaricate al trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti (distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni)¹³;
- b) osservare le regole ordinarie per ciò che attiene all'eventuale designazione di responsabili del trattamento.

L'EDPB, sul punto, nelle Linee guida non fornisce indicazioni. Ciò, probabilmente, perché si tratta di questioni "ordinarie" che attengono a qualsiasi trattamento di dati personali.

In questa direzione, le figure di riferimento, oltre – ovviamente – al Titolare, sono le seguenti:

- *Contitolare*. Nel caso di contitolarità è necessario il relativo Accordo (ex art. 26 del GDPR), con particolare attenzione all'individuazione delle attività svolte congiuntamente, ovvero individualmente e le relative ricadute, sia in termini organizzativi, che rispetto ai diritti degli interessati;
- *Responsabile esterno del trattamento*. La presenza di un responsabile, ex art. 28 del GDPR, per le attività di videosorveglianza, è una situazione abbastanza frequente, con l'obbligo – da parte del

¹³ Ad. es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, etc.

Titolare – di accertare (preventivamente ed in costanza di rapporto), la presenza ed il mantenimento dei requisiti richiesti per i trattamenti¹⁴;

- *Soggetto autorizzato (o designato) al trattamento*. La designazione dei soggetti autorizzati (art. 26 del GDPR e art. 2-*quaterdecies* del Codice privacy) rientra tra le misure organizzative del Titolare e richiede una specifica formazione, sia essa in termini generali sulla videosorveglianza, che con riferimento alle specifiche attività e procedure di trattamento svolte nell'ente;
- *Amministratore di Sistema*. Questo soggetto può essere esterno (ed allora valgono le indicazioni di cui all'art. 28 del GDPR), ovvero interno (ed allora è uno dei soggetti "autorizzati"). Si applicano le disposizioni in materia di Amministrazione dei Sistemi, con le specificazioni riguardanti anche la gestione del sistema di videosorveglianza.

La "preposizione" al trattamento (a parte il caso di contitolarità e di nomina del Responsabile esterno), segue l'attribuzione delle competenze 'funzionali' ascritte nella declinazione dell'assetto organizzativo dell'Ente che, per le funzioni "privacy", è anche noto con l'espressione "Organigramma privacy".

Infine, va ricordato il ruolo del RPD/DPO che, anche sulla videosorveglianza, assiste il Titolare (o Contitolare) nel rispetto delle disposizioni vigenti.

2.6.2. – B) Misure di sicurezza tecniche ed organizzative

Com'è noto il GDPR impone l'adozione, da parte del Titolare, di misure tecniche ed organizzative *adeguate* ai trattamenti che intende svolgere. La valutazione dell'adeguatezza è svolta preventivamente, ossia prima di effettuare il trattamento di dati personali.

Tra le principali disposizioni del GDPR si ricordano, al riguardo, le seguenti:

- il Titolare deve essere in grado di dimostrare la conformità del trattamento a quanto richiesto dal GDPR (art. 24);
- i dati personali devono essere protetti, in modo efficace, sin dalla progettazione del trattamento affinché, nello svolgimento del medesimo, siano già assicurati profili di tutela dell'interessato (art. 25, riguardo la *privacy by design*);
- i dati personale trattati devono essere solo quelli necessari per conseguire ogni specifica finalità di trattamento e l'impostazione predefinita del trattamento deve garantire la tutela degli interessati (art. 25 cit., riguardo la *privacy by default*);
- deve essere garantito un livello di sicurezza adeguato al rischio rispetto ai diritti e le libertà delle persone fisiche (art. 32).

Rispetto alle misure tecniche, le Linee guida dell'EDPB indicano quanto segue.

Le specifiche e la progettazione del sistema – ancor prima che venga messo in produzione - dovrebbero includere requisiti per il trattamento dei dati personali conformemente ai principi di cui all'art. 5, del GDPR.

Nel caso in cui un titolare preveda di acquistare un sistema di videosorveglianza commerciale, **deve includere questi requisiti nelle specifiche di acquisto**.

È necessario proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la **conservazione** (dati a riposo), la **trasmissione** (dati in transito) e l'**utilizzo** (dati in uso).

Vanno inoltre privilegiati sistemi che:

¹⁴ Le Linee guida dell'EDPB raccomandano al Titolare di inserire, nelle specifiche inerenti l'acquisto (o, comunque, la disponibilità) di un sistema di videosorveglianza, idonee clausole contrattuali inerenti il rispetto dei principi di *privacy by design* e di *privacy by default*, nel rispetto dei principi di cui all'art. 5 del GDPR. Il Titolare deve fare in modo di garantire – anche con la collaborazione del Responsabile – che la conformità al GDPR si applichi a tutti i componenti del sistema ed ai dati trattati, durante l'intero ciclo di vita del sistema e dei trattamenti.

- consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure l'editing di immagini di terzi, quando si forniscono filmati agli interessati;
- non dispongano di funzioni non necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, radiotrasmissione, analisi e registrazioni audio);
- siano conformi a standard e specifiche tecniche per i sistemi multimediali (Ad es.: IEC TS 62045 – Sicurezza multimediale – Linee guida per la protezione della privacy di apparecchiature e sistemi in uso e fuori uso).

Prov. Garante	Linee guida EDPB
a) configurazione di diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, i soggetti che accedono devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti, solo le operazioni di propria competenza	a) definizione e applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso b) attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica
b) Implementazione di misure tecniche od organizzative per la cancellazione integrale , possibilmente in forma automatica , delle registrazioni, allo scadere del termine previsto	c) utilizzo di meccanismi di cancellazione automatici
c) Implementazione di sistemi di protezione contro i rischi di accesso abusivo (firewall/antivirus...)	d) utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici
d) nel caso di trasmissione tramite rete pubblica (internet), applicazione di tecniche crittografiche ; similmente per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs).	e) cifratura dei dati f) protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione;
	g) registrazione e revisione periodica delle azioni eseguite dagli utenti (log)
	h) esecuzione di monitoraggio e individuazione di guasti e risoluzione in tempi brevi delle carenze individuate (es., ripristino dati)

Quanto alle misure di sicurezza, sul versante organizzativo, la comparazione (e integrazione) tra le indicazioni del Garante e dell'EDPB, fornisce il quadro di seguito rappresentato.

Prov. Garante	Linee guida EDPB
	Oltre alla eventuale necessità di una DPIA (cfr. più avanti), il titolare del trattamento dovrebbe adottare un

piano di gestione appropriato, stabilire e applicare politiche e procedure relative alla videosorveglianza.

- a) limitare la possibilità, per i soggetti abilitati, di **visionare** non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare operazioni di cancellazione o duplicazione
- b) nel caso di **interventi di manutenzione**, limitare la possibilità di accesso alle immagini ai soggetti preposti (e solo se indispensabile per eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini)

Il piano dovrebbe considerare i seguenti elementi:

- definizione delle **responsabilità della gestione** e del funzionamento del sistema di videosorveglianza
- finalità e ambito di applicazione del progetto di videosorveglianza
- utilizzo appropriato e vietato (ad es.: dove e quando la videosorveglianza è consentita e dove e quando non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video)
- misure relative alla **trasparenza** (informative)
- modalità e **durata delle registrazioni video**
- **formazione** specifica per gli autorizzati
- specifiche istruzioni per la gestione:
- degli **accessi interni** alle registrazioni video e per quali scopi
- delle richieste di **accesso esterne** (esercizio diritti)
- dei **problemi tecnici e procedure di recupero**
- delle **violazioni di dati personali**

L'EDPB affronta anche il tema della sicurezza c.d. "fisica", al fine di proteggere le apparecchiature (e, quindi, i dati in esse contenuti) da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e da danni accidentali.

Tra le misure suggerite:

- tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video devono essere **protetti contro l'accesso fisico** non autorizzato;
- il **posizionamento dei monitor** (soprattutto quando si trovano in zone aperte, come una reception) deve consentire solo agli operatori autorizzati di poter visualizzare le immagini.

PRINCIPALI MISURE TECNICHE ED ORGANIZZATIVE IN MATERIA DI VIDEOSORVEGLIANZA SECONDO LE INDICAZIONI DELL'EDPB	
---	--

MISURE ORGANIZZATIVE	
----------------------	--

<i>Politiche e procedure</i>	
------------------------------	--

- | | |
|--|--|
| | <ul style="list-style-type: none">– individuare ruoli e responsabilità della gestione e del funzionamento del sistema di videosorveglianza;– stabilire e documentare le finalità e l'ambito di applicazione del sistema di videosorveglianza;– identificare gli impieghi consentiti e quelli vietati (ad esempio, uso di telecamere nascoste e registrazione audio oltre che video, riprese nei bagni, etc.);– adottare misure per garantire la trasparenza e gli obblighi di |
|--|--|

	informazione; – definire le modalità e la durata delle registrazioni video, compresa la conservazione delle videoregistrazioni; – definire un piano della formazione specifica; – individuare le regole di autorizzazione all’accesso alle registrazioni e per quali finalità; – stabilire le procedure operative della videosorveglianza (ad esempio, da chi e da dove viene monitorata la videosorveglianza), – definire le procedure che devono seguire i soggetti esterni per richiedere le videoregistrazioni e le procedure per accogliere o respingere tali richieste; – definire le modalità operative a seguito dell’accoglimento delle richieste di accesso da parte di soggetti esterni; – stabilire le procedure per l’approvvigionamento, l’installazione e la manutenzione del sistema di videosorveglianza; – stabilire dal punto di vista organizzativo le procedure per la gestione degli incidenti e del data breach; – definire dal punto di vista organizzativo le procedure di continuità operativa e di data recovery.
MISURE TECNICHE	
<i>Sicurezza del sistema e dei dati</i>	– assicurare la protezione dell’intera infrastruttura della videosorveglianza (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti; – gestire la protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione; – adottare sistemi di crittografia delle immagini; – adottare soluzioni hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici; – adottare sistemi di monitoraggio su malfunzionamenti di hardware, software e interconnessioni; – adottare procedure tecniche per ripristinare la disponibilità dei dati personali e l’accesso agli stessi in caso di incidenti fisici o tecnici.
<i>Controllo degli accessi</i>	– adottare misure fisiche e logiche per consentire, ai soli soggetti legittimati, l’accesso ai locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in quelli in cui vengono conservate le riprese video; – definire le procedure per la concessione, la modifica e la revoca dei permessi di accesso fisico e logico; – curare che il posizionamento dei monitor (soprattutto quando si trovano in zone aperte, come una reception) consenta la visualizzazione ai soli operatori autorizzati; – verifica dei log e degli accessi fisici e soluzione delle carenze individuate.

2.7. – TEMPI DI CONSERVAZIONE

I dati personali oggetto di trattamento non devono essere conservati per un periodo superiore a quello necessario al conseguimento delle finalità del trattamento (art. 5, del GDPR). Questo principio vale anche per le immagini acquisite mediante sistemi di videosorveglianza.

L'EDPB ha stabilito che la tempistica della conservazione delle immagini dovrebbe essere valutata in termini **il più possibile ristretti**. In via generale, gli scopi legittimi della videosorveglianza sono spesso la protezione del patrimonio o la conservazione di elementi di prova ed è solitamente possibile individuare eventuali danni **entro uno o due giorni**.

Conseguentemente i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve allo scopo di rilevare atti vandalici) – cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici.

Le indicazioni del Garante, quindi, su un periodo (massimo) di 7 giorni, non sono più cogenti.

Questo, tuttavia, non significa che non sia ammissibile la conservazione per un periodo superiore a 24-48 ore se siano accuratamente esplicitate le motivazioni inerenti lo scopo e la necessità di una conservazione per un periodo superiore.

2.8. – DIRITTI DEGLI INTERESSATI

L'EDPB ha fornito alcune indicazioni in relazione ai diritti degli interessati, con riferimento ad alcune fattispecie.

Diritto di accesso:

- non esercitabile per i trattamenti senza conservazione (monitoraggio in tempo reale);
- nel caso di richiesta di immagini in cui siano presenti anche terzi, si dovrebbero mettere in atto misure tecniche per soddisfare la richiesta di accesso, ad es. modifica delle immagini tramite mascheramento o cifratura;
- nel caso in cui il Titolare non sia in grado di identificare l'interessato che presenta richiesta, dovrebbe avviare una interlocuzione chiedendo che sia specificato nel modo più preciso possibile quando il soggetto è entrato nella zona di ripresa e/o ulteriori elementi utili all'evasione della richiesta;
- nel caso di cui al punto precedente, ove la richiesta non sia circostanziata e quindi possa essere ritenuta «eccessiva» (art. 12, del GDPR) il Titolare potrebbe addebitare un costo ragionevole all'interessato;
- se sono trascorsi i tempi di conservazione (e, quindi, le immagini sono state cancellate) l'interessato deve essere informato della circostanza.

Diritto alla cancellazione:

- conferma l'applicabilità delle eccezioni previste dall'art. 17 (tra cui: il trattamento è effettuato per un obbligo legale o interesse pubblico);
- la richiesta potrebbe essere assolta offuscando l'immagine dell'interessato, senza alcuna possibilità di recuperare successivamente i dati personali precedentemente contenuti¹⁵.

¹⁵ Per rendere l'immagine non identificabile si adoperano, in genere, due tecniche: il c.d. "bleraggio" ed il c.d. "pixellaggio".

"Blerare" – che deriva dai verbi inglesi *to blear* (offuscare, sfocare) o *to blur* (annebbiare) – indica l'azione di 'offuscamento' delle immagini (si pensi ai volti dei minori o ai marchi d'impresa). Con il termine "Pixellare" (da pixel) s'intende, in un'immagine

Diritto di opposizione:

- vantabile in relazione a trattamenti posti in essere sulla base dell'interesse pubblico (e dell'interesse legittimo);
- prevede l'astensione del Titolare dal trattare i dati dell'interessato, salvo che non dimostri l'esistenza di motivi legittimi cogenti che prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato deve vantare e addurre «motivi connessi alla sua situazione particolare» (ad es., particolari circostanze che potrebbero rivelare opinioni politiche o religiose, in grado di ledere i suoi interessi);
- in relazione alla videosorveglianza, l'accoglimento della richiesta potrebbe esplicitarsi nello spegnimento immediato della telecamera, per il tempo necessario a non riprendere l'interessato.

2.9. – VALUTAZIONE SULLA NECESSITA' DI EFFETTUARE UNA DPIA

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza potevano essere effettuati rispettando le misure e gli accorgimenti prescritti dall'Autorità ad esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (art. 17 del previgente Codice privacy).

La verifica preliminare era prevista quando vi fossero rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare. Ora detta verifica non è più prevista se non ad esito di una DPIA che attesti un rischio elevato per gli interessati (consultazione preventiva, ex art. 36 del GDPR).

Secondo l'art. 35 del GDPR, «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi (...).

La valutazione d'impatto (...) è richiesta in particolare nei casi seguenti:

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati (...).

Il WP29 – ora EDPB – nelle *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del*

digitalizzata, “mascherare e rendere indistinguibile o irricognoscibile, mediante l'ingrandimento sproporzionato dei pixel, una scena, un particolare, o, molto spesso, il volto di una persona, specialmente se minorenne” (Dizionario Treccani).

Nonostante l'obiettivo identico le risultanze delle due tecniche possono dare risultati diversi a seconda, rispettivamente, del livello di offuscamento o di pixelaggio. Uno sfocamento estremo è generalmente irrecuperabile, il pixelaggio può invece essere “recuperato” mediante specifici software.

*regolamento (UE) 2016/679*¹⁶ ha identificato 9 criteri in presenza dei quali il trattamento potrebbe presentare un livello di “rischio inerente” potenzialmente elevato (in neretto si evidenziano i criteri applicabili, a seconda dei casi, alla videosorveglianza):

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione;
2. processo decisionale automatizzato che ha effetti giuridici o incida in modo analogo significativamente sui diritti degli interessati;
3. **monitoraggio sistematico;**
4. dati sensibili o dati aventi carattere altamente personale;
5. trattamento di dati su larga scala;
6. creazione di corrispondenze, combinazione o messa in relazione di due o più insiemi di dati;
7. **dati relativi a interessati vulnerabili;**
8. **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;**
9. impedimento agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Le Linee guida EDPB sulla videosorveglianza, oltre a richiamare il quadro normativo di cui sopra, specificano che, date le finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione biometrica di soggetti sospetti), è ragionevole supporre che molti casi di videosorveglianza richiederanno una valutazione d’impatto sulla protezione dei dati. I Titolari del trattamento dovrebbero quindi consultare l'elenco delle tipologie di trattamento soggette obbligatoriamente a valutazione d’impatto predisposte dalle Autorità nazionali, ai sensi dell'art. 35, par. 4, del GDPR.

Con il Provv. 11 ottobre 2018, n. 467, il Garante ha disposto l’«**Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d’impatto sulla protezione dei dati**»

Le tipologie di trattamento indicate - redatte sulla base delle Linee guida WP 248 *ed allo scopo di specificarne ulteriormente il contenuto e a complemento delle stesse* - comprendono, tra gli altri:

- **monitoraggio sistematico**, utilizzato per osservare, monitorare o controllare gli interessati: questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);
- **dati relativi a interessati vulnerabili**: il trattamento di questo tipo di dati è un criterio legato all'aumento dello squilibrio di potere tra gli interessati (dipendenti) e il Titolare del trattamento);
- **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**: quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, etc.

Per l’effettuazione della DPIA, la Camera di Commercio di Reggio Calabria dispone di un documento specifico, al quale si rinvia.

Qualora il sistema di videosorveglianza sia già in esercizio, il Titolare deve verificare se sia necessario effettuare una DPIA. In ogni caso nella propria valutazione, potrà acquisire le informazioni eventualmente provenienti dalla valutazione d’impatto (o dalla documentazione tecnica) preparata dal fornitore del prodotto.

¹⁶ WP 248 rev del 4 ottobre 2017.

Si tratta di un aspetto importante perché la DPIA del fornitore (o analogo documento) potrà contenere dettagli in merito alla innovatività delle tecnologie utilizzate, alle misure di sicurezza presenti nel dispositivo tecnologico oggetto della valutazione del Titolare utilizzatore che, quindi, se opportunamente configurato, gli consentirà una adeguata gestione dei rischi e la dimostrazione del rispetto dei principi della *privacy by design* e *by default*, anche in assenza della formalizzazione di una apposita DPIA.

Si ricorda, al riguardo, che il Responsabile esterno del trattamento è tenuto a collaborare con il Titolare posto che l'art. 28, par. 3, lett. f), del GDPR, prevede che detto responsabile "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

2.10. – LE SANZIONI

Anche sulla videosorveglianza si applicano le sanzioni:

- a) amministrative pecuniarie, previste dagli artt. 82 e 83, del GDPR;
- b) penali ed amministrative previste dal Codice privacy.

In tale ambito, le sanzioni riguardano, solitamente, le seguenti fattispecie:

- inosservanza dei principi generali di trattamento dei dati;
- carente o insufficiente adempimento degli obblighi di informazione;
- trattamento illecito per mancanza di una idonea base giuridica per il trattamento dei dati.

Considerato che il presente Disciplinare non riguarda la videosorveglianza dei lavoratori, si omettono le indicazioni sullo specifico regime sanzionatorio previsto dalla disciplina vigente.

In relazione alle sanzioni occorre interrogarsi sulla valenza delle indicazioni contenute nelle Linee guida dell'EDPB e se la loro violazione/inosservanza da parte del Titolare comporti l'applicazione di sanzioni.

In via di principio, i sopra citati artt. 82 e 83 non indicano tra le violazioni, le disposizioni adottate dall'EDPB. Tuttavia, l'art. 70 del GDPR stabilisce che le Linee guida del Comitato promuovono "l'applicazione coerente del presente Regolamento" hanno, cioè, natura interpretativa. Questa natura interpretativa riverbera i suoi effetti con riferimento, in particolare, all'obbligo del Titolare, ex art. 5, par. 1, lett. a), del GDPR, di trattare i dati personali dell'interessato "in modo lecito, corretto e trasparente". Il Comitato, con le sue valutazioni, concorre infatti all'applicazione "corretta" del GDPR, come indicato nell'art. 70, par. 1, lett. a).

Le conseguenze che si ravvisano sono, pertanto, le seguenti:

- a) il rispetto da parte del Titolare delle indicazioni dell'EDPB fa presumere, fatte salve le valutazioni da parte dell'Autorità di controllo e di quella giudiziaria, la correttezza del trattamento;
- b) il non rispetto delle indicazioni dell'EDPB, non costituisce prova della non correttezza, ma richiede una esplicita motivazione da parte del Titolare circa le modalità e le soluzioni adottate per i trattamenti svolti e la loro adeguatezza a quanto richiesto dal GDPR.

3 - PARTE II – ORGANIZZAZIONE

3.1. - MODELLO ORGANIZZATIVO PRIVACY

3.1.1. – Titolare e Contitolare

Il Titolare del trattamento è la Camera di commercio di Reggio Calabria, con sede legale in Via Tommaso Campanella n. 12.

Secondo gli ordinari criteri di imputazione della volontà dell'Ente, il soggetto deputato, in relazione al presente trattamento, ad esprimere la volontà del Titolare è il Segretario Generale.

Per esercitare in concreto i suoi poteri, il Titolare si avvale delle figure individuate ai punti successivi.

Non si possono escludere situazioni di contitolarità, qualora vi siano – nel complesso dei locali della Camera di commercio – altri soggetti autonomi che condividono le esigenze e la strumentazione della videosorveglianza¹⁷.

Per la predisposizione di un accordo di contitolarità si rinvia a quanto indicato nelle apposite Linee guida approvate dalla Camera di commercio.

3.1.2 . – Designazione del Responsabile esterno del trattamento

L'operatore economico aggiudicatario del servizio Reception, in relazione alle immagini live che transitano sul monitor della postazione di portineria, opera in qualità di Responsabile ex art. 28 del GDPR, secondo le istruzioni impartite dal Titolare formalizzate nel relativo atto di nomina e nel rispetto delle modalità di esecuzione dei servizi, stabilite nel contratto e relativo capitolato. I compiti del Responsabile designato sono individuati nella nomina in allegato all'incarico relativo allo svolgimento delle attività di videosorveglianza.

Per la nomina del Responsabile si rinvia a quanto indicato nelle apposite Linee guida approvate dalla Camera di commercio. Un esempio è comunque riportato nell'Allegato 1.

3.1.3 – Soggetti e personale autorizzato al trattamento

I soggetti autorizzati al trattamento sono:

¹⁷ In talune occasioni, può capitare di svolgere la videosorveglianza in regime di contitolarità con altro Titolare al quale la Camera di commercio può essere legata per altre ragioni o vincoli contrattuali o giuridici di altro genere. Ad esempio, una Camera di commercio proprietaria di un immobile ad uso uffici che utilizza solo parzialmente, per una propria sede secondaria e per altri uffici utilizzati da soggetti del sistema camerale, può cedere con apposito contratto (ad es. di comodato d'uso gratuito) una o più porzioni di tale immobile anche ad un'Autorità pubblica per l'espletamento delle proprie attività istituzionali.

In tali casi, può accadere che sia la Camera che l'Autorità pubblica interessata che occupano porzioni di uno stesso immobile abbiano l'interesse comune di avviare e svolgere, ognuno per le proprie finalità istituzionali, anche congiuntamente, una attività di videosorveglianza. In detti casi, ove si decida di svolgere congiuntamente tale attività, è necessario stipulare un accordo di Contitolarità, ex art. 26 del GDPR, per determinare congiuntamente le finalità, i mezzi del trattamento e le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR per la Camera di commercio e dal D.Lgs. n. 51/2018.

Tali casistiche presentano peculiarità particolari derivanti dal fatto che la base giuridica su cui si fonda il medesimo trattamento (la videosorveglianza) di dati personali è ovviamente diversa per i due Contitolari, stante il fatto che gli stessi hanno una natura giuridica diversa e una fonte normativa differente anche se con molte similitudini. Tali situazioni, pur se non frequenti, possono presentarsi e, in tal caso, i due Contitolari devono analizzare e valutare attentamente la situazione concreta, definire congiuntamente dopo la finalità condivisa (anche se ciascuna parte la persegue per le proprie finalità istituzionali che sono diverse) anche i mezzi del trattamento, distinguendo precisamente i compiti di ciascuna parte e le rispettive responsabilità che devono comprendere, fra l'altro, le funzioni di comunicazione delle informazioni agli interessati e la procedura per l'esercizio dei loro diritti che, in tali casi, non può non tenere conto della differente natura giuridica dei Contitolari e delle diverse fonti normative che rendono legittima la medesima attività.

- a) in forza del contratto per l'affidamento del servizio di Reception, e con riferimento alle sole immagini live che transitano sul monitor della postazione di portineria, gli operatori del Responsabile Esterno al Trattamento di cui al punto 3.1.3 presenti sul sito di rischio. Il Responsabile esterno designato predispone, custodisce e mette a disposizione della Camera di Commercio, un elenco nominativo dei propri operatori.
- b) Il personale della Camera di Commercio (dipendenti e collaboratori) soggetti all'autorità diretta del Titolare, da quest'ultimo autorizzati in ragione del loro ruolo o funzione all'interno dell'Ente.

Tenuto conto del quadro sopra delineato, a tali soggetti autorizzati sono affidati i seguenti compiti che si configurano anche come trattamenti:

- a. visione delle immagini in tempo reale;
- b. accesso visivo al registrato, nei casi consentiti;
- c. possibilità di realizzazione di copie di sicurezza, autorizzate dal Titolare;
- d. presidio delle richieste di esercizio dei diritti dell'interessato, a norma degli artt. 15 ss., del GDPR, ferma restando la facoltà degli interessati di adire direttamente il DPO della Camera di commercio, i cui dati di contatto sono riportati nell'informativa fornita agli stessi;
- e. informazione verbale e/o consegna dell'informativa dettagliata ex art. 13 del GDPR.

I trattamenti specifici per la ricerca di immagini e/o per la realizzazione di copie sono attività riservate al Titolare del trattamento, nella figura del Segretario Generale. Sotto la supervisione del Segretario Generale, e previa autorizzazione dello stesso, le attività materiali di ricerca ed estrazione delle immagini può essere effettuata da altro personale della Camera di Commercio (dipendenti e collaboratori) in possesso di idonee competenze tecniche.

3.1.4. – Amministratore di Sistema

Qualora si ravvisasse la necessità, ai sensi dall'art. 28, par. 2, del GDPR, la Camera di Commercio potrebbe affidare l'incarico di Amministratore di Sistema ad una impresa specializzata anche al fine di realizzare le seguenti attività:

- a) configurazione e manutenzione degli impianti, compresa la creazione, la configurazione e la gestione tecnica dei profili utente;
- b) configurazione del sistema automatico di conservazione massima dei dati (immagini) registrati;
- c) adozione delle misure di sicurezza logiche a protezione delle immagini e della loro trasmissione in remoto.

I termini di svolgimento dell'incarico saranno oggetto di apposito disciplinare.

4 - PARTE III – REGOLAMENTO DELLA VIDEOSORVEGLIANZA

4.1. – REGOLAMENTO PER LA VIDEOSORVEGLIANZA

4.1.1. – Principi fondamentali

Con il servizio di videosorveglianza con registrazione, il Titolare intende adottare una misura volta a migliorare la sicurezza delle aree (interne o esterne) di sua pertinenza, assicurando la protezione delle persone e del patrimonio dell'Ente, materiale ed informativo, tenuto conto della sensibilità del sito di rischio in ragione dell'alto valore delle risorse che vi sono concentrate.

L'attività di videosorveglianza non sostituisce né è complementare rispetto all'attività degli organi giudiziari o di polizia giudiziaria o delle forze armate o di polizia. L'utilizzo del sistema e delle registrazioni non deve prescindere dalle normative in vigore riguardanti i compiti degli Organi di Pubblica Sicurezza, di modo che la complementarietà del sistema si limiti a permettere l'attivazione delle Forze dell'Ordine, anche se col tramite del Titolare e dei suoi collaboratori (ad es. l'Istituto/la società/Altro di Vigilanza designato Responsabile esterno).

Il trattamento dovrà pertanto avvenire nel rispetto dei seguenti principi:

1. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art. 5, lett. b), del GDPR).
2. I dati raccolti non possono essere utilizzati per finalità diverse o ulteriori e non possono essere diffusi o comunicati a terzi, salvo concrete esigenze di polizia o di giustizia.
3. Vanno rispettati 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 e stabilendo la localizzazione delle telecamere e le relative modalità di ripresa (art. 5, lett. c), del GDPR).
4. Gli interessati devono poter conoscere esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti, esercitando i diritti di cui agli artt. 15 ss. del GDPR.
5. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni di dettaglio, necessarie ai sensi dell'art. 13 del GDPR. L'informativa breve è affissa in prossimità delle aree oggetto di videosorveglianza e prima che l'interessato entri in dette aree.
6. L'informativa estesa è resa disponibile, secondo quanto indicato nell'informativa breve.
7. Occorre rispettare il divieto di controllo a distanza dei lavoratori e le garanzie previste al riguardo (art. 4, L. 300/1970, come modificato dal D.Lgs. n. 151/2015 (attuativo del c.d. *Jobs Act* L. n. 81/2015)).
8. Occorre determinare il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, rispettando i tempi e le condizioni di legge. Gli interessati dovranno essere informati sui tempi di conservazione stabiliti dal Titolare anche al fine di poter esercitare i diritti loro attribuiti dal GDPR.
9. Occorre individuare, formare, autorizzare e istruire i soggetti che possono utilizzare gli impianti e prendere visione delle registrazioni, adottando procedure atte a garantire - secondo profili diversificati - l'accesso e la realizzazione di copie esclusivamente ai soggetti autorizzati. Tali soggetti sono in numero limitato, nominativamente identificati e dotati in via preventiva di specifici profili di autorizzazione, tali da consentire l'esecuzione delle sole operazioni necessarie e sufficienti all'assolvimento dei loro compiti. Sono soggetti all'autorità diretta del Titolare oppure del Responsabile esterno designato, secondo l'organizzazione di appartenenza e gli incarichi assegnati. Il personale è vincolato al segreto professionale.
10. I tecnici installatori e manutentori del sistema ed il personale tecnico informatico (in qualità di Amministratori di Sistema) potranno avere accesso ai sistemi per garantirne il corretto funzionamento. Essi possono avere accesso alle immagini solo se ciò è indispensabile, nei limiti ed in ragione delle

operazioni che devono compiere. Il personale è vincolato al segreto professionale. Il Titolare, oppure il Responsabile esterno designato, secondo l'organizzazione di appartenenza e gli incarichi assegnati, dovranno redigere e tenere aggiornata la loro lista nominativa, anche in considerazione della loro funzione di Amministratore di Sistema, ai sensi delle Linee guida approvate dalla Camera di commercio, in relazione al GDPR ed al Prov. del Garante 27 novembre 2008.

11. L'accesso visivo alle immagini, la loro registrazione e la loro trasmissione in rete deve essere protetta da misure di sicurezza idonee ad evitare ogni rischio di perdita, distruzione, accesso non autorizzato, trattamento illegittimo, non corretto o non conforme alle finalità dichiarate. In particolare, l'uso di apparati e sistemi digitali collegati in remoto, anche via wireless, devono implementare le misure di sicurezza richieste dalla normativa vigente, come specificate dal vigente Provvedimento del Garante e dalle Linee guida dell'EDPB.
12. Gli impianti dovranno essere configurati in modo da ridurre al minimo l'impatto sulla riservatezza degli interessati. Pertanto, non dovranno essere modificati gli angoli di ripresa o la definizione delle immagini, se non nel caso in cui ciò sia indispensabile a fronte di eventi anomali. Le funzionalità dei sistemi di controllo software devono essere configurate in modo che il loro impiego non risulti eccedente rispetto alla normale attività di videosorveglianza.

4.1.2. – Finalità del trattamento

La Camera di commercio di Reggio Calabria effettua attività di videosorveglianza esclusivamente per garantire la sicurezza del patrimonio dell'Ente e delle persone che, a vario titolo, frequentano gli ambienti delle strutture o che accedono agli stessi.

In particolare, il controllo delle aree assicura:

- A. l'individuazione e la gestione delle aree e dei punti strategici afferenti alla sicurezza;
- B. la tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo e terrorismo, improvvisi ed imprevedibili;
- C. il monitoraggio e la rilevazione - in supporto al sistema di teleallarme - di eventuali situazioni di pericolo a protezione dell'incolumità delle persone, delle proprietà e del patrimonio dell'Ente per le quali, ricorrendo una effettiva esigenza di deterrenza a fronte di un rischio elevato, altre misure di protezione non sono sufficienti, non sono attuabili (per es. per il loro costo) o non sono parimenti efficaci.
- D. La rilevazione e la prevenzione di situazioni di pericolo nelle aree in cui possono essere presenti i lavoratori, al fine di consentire l'intervento delle squadre di emergenza, dei mezzi di soccorso e degli addetti alla sicurezza, nel rispetto della normativa vigente;

I dati trattati e raccolti mediante i sistemi di videosorveglianza con videoregistrazione, potranno essere utilizzati in sede di un eventuale giudizio civile o penale, per agevolare l'esercizio del diritto di difesa da parte del Titolare del trattamento.

4.1.2.1 – Esclusioni e divieti

Costituiscono esclusioni e divieti i seguenti:

- a) A tutela dei lavoratori, è **vietato il trattamento delle immagini per qualunque finalità di controllo sull'attività dei lavoratori**¹⁸.

¹⁸ La specificazione è necessaria poiché se il sistema di videosorveglianza riprende anche i lavoratori (es., in entrata/uscita), questo trattamento, che può risultare 'fisiologico', non può essere utilizzato in alcun modo ai fini del controllo sull'attività dei suddetti lavoratori, per il quale è necessario un diverso approccio disciplinare, secondo quanto previsto, in particolare, dall'art. 4 della legge n. 300/1970. Si veda, inoltre, l'art. 88 del GDPR e l'art. 111 del Codice privacy.

- b) Si esclude il trattamento per il perseguimento di finalità private e personali. Fatto salvo l'esercizio dei diritti dell'interessato, a norma degli artt. 15 ss. del GDPR e l'ordine di una Autorità, le richieste di accesso alle immagini da parte di privati (compresi i lavoratori) per la tutela di un diritto non correlato alle finalità perseguite e dichiarate dal Titolare, devono essere mediate dall'ordine di una Autorità ed autorizzate dal Titolare. E' fatto salvo il diritto degli avvocati, ai sensi dell'art. 391-*quater* del cod. proc. pen., ad avere copia delle immagini registrate (versando il costo eventualmente stabilito dalla Camera di commercio), a condizione che la richiesta motivata (anche tramite l'interessato) sia presentata in qualità di difensore di fiducia/d'ufficio dell'interessato indagato nell'ambito di un procedimento penale.

4.1.3. – Base giuridica

La base giuridica della videosorveglianza è il legittimo interesse del Titolare, ai sensi dell'art. 6, par. 1, lett. f), del GDPR. Come indicato anche nelle Linee guida dell'EDPB, tale base giuridica è legittima se necessaria per il perseguimento di uno scopo del titolare del trattamento che può derivare da un suo interesse legale, economico o non materiale.

È tuttavia necessario fare attenzione a che gli interessi del titolare non prevalgano sui diritti e le libertà fondamentali degli interessati, adottando le seguenti verifiche:

- a) Verificare e dimostrare la sussistenza dell'interesse legittimo del Titolare;
- b) Verificare e dimostrare che il trattamento dei dati personali è necessario al conseguimento dello scopo;
- c) Verificare che le modalità del trattamento non determinino una situazione di squilibrio, a svantaggio dell'interessato, in relazione ai suoi diritti e libertà fondamentali.

Per quanto riguarda la lett. a), ad esempio, la tutela della proprietà e dei beni, nel caso delle Camere di commercio, può avere una diretta relazione con la tutela di beni di valore storico, artistico, etc., ovvero con la tutela delle persone fisiche siano essi i lavoratori che gli utenti dei servizi.

Rispetto alla lett. b), l'utilizzo della videosorveglianza va comparato con altre possibili soluzioni (esempio: un servizio di "ronda" con guardie private), evidenziandone anche l'incidenza in termini di costo per il Titolare.

Per quanto riguarda la lett. c), la videosorveglianza deve essere coerente con le esigenze del trattamento. Si pensi a telecamere di ampio raggio, con qualità di ripresa ad alta definizione, ovvero con la registrazione anche dell'audio, o, ancora, con meccanismi di riconoscimento biometrico, etc.

4.2 – MODALITÀ DI TRATTAMENTO

4.2.1. – Descrizione dell'impianto

Il sistema di videosorveglianza è composta da n. 6 telecamere a presidio delle aree di seguito precisate:

1. una telecamera fissa posizionata all'interno della sala multimediale a copertura del portone della CCIAA sito in Via Logoteta;
2. una telecamera fissa posizionata all'esterno a copertura del portone della CCIAA sito in Via Logoteta;
3. una telecamera fissa posizionata al piano terra a presidio della porta di vetro interna, nei pressi del corridoio retro sportelli utenti, dalla quale si ha accesso ad altri uffici camerali;
4. una telecamera fissa posizionata all'esterno della sede camerale nel cortile di Via Furnari a copertura delle porte di accesso all'Ente;

5. una telecamera fissa posizionata all'esterno della sede camerale a copertura del portone secondario dell'Ente sito in Via Furnari;
6. una telecamera fissa posizionata all'esterno della sede camerale a copertura del portone principale dell'Ente sito in Via Tommaso Campanella;

4.2.2. – Accesso logico

Le telecamere sono collegate ad un apparato DVR (digital video recorder - registratore video digitale) posizionato al piano terra presso la sala server che è chiusa a chiave ed è accessibile esclusivamente al personale autorizzato. Le immagini provenienti dall'impianto di videosorveglianza sono visualizzabili attraverso un monitor posizionato al piano terra presso la postazione del personale che gestisce l'accesso alla sede camerale (portineria). Il personale addetto all'ingresso può unicamente visionare le immagini in tempo reale, non è invece abilitato ad effettuare fermi immagine o a riprodurre nuovamente le immagini.

Le immagini sono conservate per un periodo pari a 24 ore. Trascorso tale periodo, le immagini vengono automaticamente sovrascritte dal sistema.

Per accedere alle immagini in tempo reale o registrate è necessario autenticarsi al sistema con specifiche credenziali di accesso.

4.2.3. – Collegamento da remoto alla centrale di controllo del Responsabile

Le immagini non sono accessibili da remoto.

4.3. – DATA PROTECTION IMPACT ASSESSMENT (DPIA)

4.3.1. – Data Protection Impact Assessment (DPIA)

Quando un tipo di trattamento che prevede, in particolare, l'uso di nuove tecnologie può presentare, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare, **prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA), a norma degli artt. 35 e 36 del GDPR.

La DPIA rappresenta un'autonoma valutazione che il Titolare del trattamento effettua per analizzare la necessità, la proporzionalità e i rischi di un determinato trattamento di dati per i diritti e le libertà delle persone fisiche. È importante per tutti quei trattamenti dati raccolti tramite la videosorveglianza che possono rappresentare un rischio *elevato* per i diritti e le libertà degli interessati.

L'art. 35, par. 3, lett. c), del GDPR richiede, pertanto, la conduzione di una valutazione di impatto in caso di videosorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Per valutare se un trattamento è svolto su larga scala si deve far riferimento al numero degli interessati, al volume di dati e/o tipologie di dati, alla durata dell'attività di trattamento e all'ambito geografico dell'attività di trattamento. In altri termini, nei casi in cui il titolare tratta dati particolari su larga scala, è tenuto a svolgere una valutazione d'impatto.

Nei casi in cui la Camera di commercio volesse prevenire reati connessi alla proprietà, invece di installare un sistema di videosorveglianza, potrebbe, piuttosto, adottare misure di sicurezza alternative come recintare la proprietà, impiegare pattuglie regolari del personale di sicurezza, utilizzare portieri/custodi, dotare i locali e gli spazi di una migliore illuminazione, installare serrature di sicurezza, finestre e porte a prova di manomissione o applicare rivestimenti antigraffiti o lamine alle pareti. Tali misure possono essere efficaci quanto i sistemi di videosorveglianza contro furto con scasso, furto e atti vandalici.

Prima di utilizzare un sistema di telecamere, pertanto, la Camera di commercio è tenuta a valutare quando e dove le misure di videosorveglianza sono strettamente necessarie. Di solito un sistema di sorveglianza che funziona di notte e al di fuori del normale orario di lavoro può soddisfare, in numerosi casi, le esigenze della Camera di commercio/Titolare del trattamento per prevenire pericoli per il proprio patrimonio immobiliare e di altro genere.

In ogni caso, la DPIA dovrà riportare:

1. la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento (ovvero altra base giuridica se applicabile);
2. la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. la valutazione dei rischi per i diritti e le libertà degli interessati;
4. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Pertanto, ove il Titolare intenda svolgere un trattamento di videosorveglianza per i propri beni e a tutela del proprio interesse legittimo, dovrà far svolgere una DPIA, con l'assistenza del Responsabile esterno del trattamento a norma dell'art. 28, par. 3, lett. f), del GDPR, consultando, ove lo ritenga necessario, il proprio DPO, ovvero richiedendogli un parere in merito.

La valutazione d'impatto, in ogni caso e fra l'altro, dovrà precisare che:

- a. si procede al trattamento per effettive esigenze di deterrenza a fronte di minacce improvvise e imprevedibili nel loro verificarsi, con impatto potenzialmente grave per le cose e le persone;
- b. l'elevato valore delle risorse e del patrimonio informativo da tutelare, anche a fronte del particolare e rilevante interesse pubblico perseguito dal Titolare stesso;
- c. le telecamere sono opportunamente segnalate e possono inquadrare aree interne ed esterne preventivamente individuate;
- d. la visione delle immagini registrate può avvenire solo mediante accesso fisico al DVR custodito presso la sede camerale;
- e. i dati possono essere consultati solo da personale appositamente autorizzato, previamente formato ed istruito;
- f. l'accesso da parte del personale tecnico (AdS) addetto alla configurazione ed alla manutenzione degli impianti può avvenire solo previa autorizzazione;
- g. sono stati definiti e configurati tempi massimi per la conservazione delle immagini, individuando modalità per la gestione delle eventuali copie c.d. *off-site* da realizzarsi su ordine di una Autorità (Vedi, più avanti, la Parte VI, del presente Disciplinare);
- h. sono state individuate modalità e procedure per consentire agli interessati l'esercizio dei loro diritti (Vedi, più avanti, la Parte VI, del presente Disciplinare);
- i. i sistemi di videosorveglianza non sono connessi direttamente o indirettamente con altre banche dati, anagrafiche o biometriche.

Ove dagli esiti della valutazione d'impatto svolta risulti che:

- a) sono state verificate e soddisfatte tutte le soprastanti condizioni;
- b) sia stato richiesto uno specifico parere al DPO e questo sia stato reso senza osservazioni, rilievi o richieste di adeguamento delle specifiche misure di sicurezza tecniche e organizzative illustrate nella DPIA;
- c) il trattamento non esponga - anche in ragione delle specifiche misure di sicurezza implementate e descritte nel presente disciplinare - gli interessati ad un rischio specifico per i loro diritti e le loro libertà.

Il Titolare potrà procedere al trattamento senza attivare le procedure di consultazione preventiva di cui all'art. 36 del GDPR.

Diversamente, se i risultati della DPIA indicano che il trattamento comporterebbe rischi elevati nonostante le misure di sicurezza pianificate dalla Camera di commercio, sarà necessario prima di iniziare il trattamento consultare il Garante, a norma dell'art. 36 del GDPR.

La valutazione d'impatto (ai sensi dell'art. 35, par. 11, del GDPR) dovrà essere riesaminata qualora, in caso di variazione delle caratteristiche del trattamento¹⁹, si modifichi il livello di rischio per gli interessati. Sulla base degli esiti del riesame il Titolare del trattamento valuterà l'attivazione degli adempimenti sopra richiamati, adottando nel frattempo le cautele necessarie affinché siano comunque preservati i diritti degli interessati.

Ulteriori elementi generali e procedurali sui trattamenti soggetti a tale valutazione di impatto, su come impostare, predisporre e far svolgere tale verifica preliminare sono disponibili nello specifico documento della Camera di commercio su "Procedura per la predisposizione di una valutazione di impatto dei dati personali".

4.4. – AGGIORNAMENTO DEL REGISTRO DEI TRATTAMENTI

La procedura per l'attivazione (o la revisione) della videosorveglianza richiede che tutte le relative informazioni sui trattamenti vengano riportata all'interno del Registro dei trattamenti della Camera di commercio.

4.5. – INFORMATIVA

4.5.1. – Informativa agli interessati

Gli interessati devono sempre essere informati del fatto che stanno per accedere in una zona video sorvegliata tramite apposita informativa.

A tal fine, negli ambienti e negli spazi sottoposti a videosorveglianza, la Camera di commercio installa, in posizione chiaramente visibile, prima del raggio di azione della telecamera, appositi cartelli contenenti l'informativa semplificata conforme alle indicazioni stabilite dal Garante (simbolo della presenza di telecamere, identificativo del Titolare, finalità della raccolta, etc.). In allegato è riportato un modello-tipo di tale informativa semplificata (v. Allegato 2).

Nelle reception/accoglienza viene messa a disposizione degli interessati l'informativa estesa, contenente tutti gli elementi di cui all'art. 13 del GDPR, secondo il modello riportato nell'Allegato 3.

4.5.2. – Informativa ai lavoratori. Rinvio

Il presente Disciplinare – come detto – non riguarda la videosorveglianza dei lavoratori. Non si pone, pertanto, alcuna necessità di specifica informativa ai lavoratori medesimi.

4.6. – DURATA DEL TRATTAMENTO E TERMINI DI CONSERVAZIONE DELLE REGISTRAZIONI

Determinato un livello di rischio alto, in relazione alla sensibilità ed al rilevante interesse pubblico delle attività che vi si svolgono, nonché dei beni che vi si trovano, della valutazione storica e prognostica di possibili eventi illeciti e dannosi, alla ubicazione del sito di rischio, delle caratteristiche e dei limiti tecnici del

¹⁹ Ad es., modifica della configurazione degli impianti con impatto rilevante sul trattamento, oppure implementazione di funzionalità nuove o ulteriori, ove ciò sia ritenuto indifferibile - anche su segnalazione del Responsabile esterno – per elevare lo standard di sicurezza a fronte di un aumento del livello di rischio o di una seria possibilità di verifica di nuove minacce.

sistema di videoregistrazione, il periodo di conservazione delle immagini si determina in 24 ore dalla loro rilevazione.

4.7. – ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Mediante apposita istanza in forma scritta, indirizzata al Titolare o al Responsabile designato nonché indirizzabile, in ogni caso, direttamente al DPO, anche consegnata tramite soggetti autorizzati al trattamento, l'interessato potrà esercitare i seguenti diritti:

- a. ottenere conferma o smentita dell'esistenza di immagini che lo riguardano;
- b. accedere ai dati che lo riguardano ed ottenerne copia;
- c. verificare le finalità, le modalità e la logica del trattamento;
- d. ottenerne il blocco, qualora i dati siano trattati in violazione di legge, nonché la cancellazione delle immagini registrate in difformità dagli scopi dichiarati nelle informative.

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione, in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

La risposta ad una richiesta di esercizio dei diritti riguarderà soltanto i dati attinenti al richiedente identificabile e le immagini che lo riguardano direttamente.

Di regola, l'accesso visivo alle riprese, alle registrazioni e la consegna di eventuali copie, se disponibili e tenuto conto dei tempi di conservazione delle stesse, è esclusivamente riservato alla magistratura ed alle Forze dell'ordine, nonché, come detto in precedenza, agli avvocati in caso di difesa dell'interessato in un procedimento penale.

Qualora risulti indispensabile concedere all'interessato il diritto di accedere visivamente alle immagini, se necessario dovranno essere adottate tecniche di schermatura (anche manuale) del video o programmi che rendano possibile l'oscuramento delle immagini che riprendono altri interessati.

La visione potrà comprendere eventuali dati riferiti a terzi soltanto se la scomposizione dei dati trattati o la privazione di alcuni elementi del video rendessero incomprensibili i dati personali dell'interessato.

Tutti gli accessi devono essere registrati mediante annotazione riportante data e ora dell'accesso, identificazione del richiedente, nonché gli estremi dell'autorizzazione all'accesso.

4.8. – REGOLE GENERALI DI COMPORTAMENTO DEGLI ADDETTI ALLA VIDEOSORVEGLIANZA

Di seguito sono indicate alcune regole generali di comportamento per gli addetti alla videosorveglianza:

- a) L'addetto alla sorveglianza autorizzato a raccogliere, gestire e custodire le immagini, deve agire nei limiti delle istruzioni ricevute e secondo le procedure indicate nelle disposizioni di servizio.
- b) Ove l'operatore incaricato ritenga che ciò non avvenga, non sia avvenuto o non possa avvenire, deve informarne il proprio Responsabile del trattamento diretto (nella persona del superiore gerarchico o funzionale). Il Responsabile avviserà il Titolare del trattamento al fine di adottare le misure ritenute opportune.
- c) L'accesso alle immagini deve limitarsi alle attività oggetto della sorveglianza: devono essere ignorate eventuali altre informazioni di cui si possa venire a conoscenza, osservando il comportamento di un soggetto ripreso. In particolare, non dovranno essere date informazioni di alcun genere né attivate operazioni di ricerca, estrapolazione e copia delle immagini, richieste o sollecitate telefonicamente o verbalmente.
- d) L'operatore incaricato non deve riferire a terzi estranei alcun elemento contenuto nelle immagini e nelle registrazioni o di cui comunque sia venuto a conoscenza nel corso della sua attività di sorveglianza. È altresì vietato duplicare le immagini (per es. fotografando lo schermo con il proprio

smartphone personale) e quindi diffonderle, comunicarle o consentire l'accesso a soggetti diversi da quelli individuati nel presente Disciplinare, secondo la procedura per l'accesso alle immagini, di cui al successivo paragrafo 5.2.

- e) L'operatore incaricato non ha autonomia decisionale e dovrà attenersi alle istruzioni ricevute. In caso di dubbio dovrà rivolgersi al proprio Responsabile del trattamento diretto e attendere istruzioni che devono essere fornite per iscritto.
- f) L'operatore incaricato deve custodire con diligenza le immagini eventualmente in suo possesso, applicando le istruzioni e le disposizioni di servizio ricevute, nel rispetto delle regole previste dal presente Disciplinare.
- g) L'obbligo di riservatezza non si applica ai rapporti con il Titolare né con il Responsabile esterno designato, con i superiori, con la magistratura e le Forze dell'ordine. In caso di dubbio, è fatto obbligo all'operatore incaricato di chiedere istruzioni scritte al Responsabile del trattamento di riferimento.

5 - PARTE IV – PROCEDURE DI GESTIONE

5.1. – GESTIONE DELLE IMMAGINI

5.1.1. – Trattamento delle riprese in tempo reale

Il trattamento deve essere effettuato in modo da limitare l'angolo di visuale all'area effettivamente da proteggere. Per quanto possibile, dovrà essere evitata la ripresa di luoghi circostanti e di dettagli che non risultino rilevanti (Principio della minimizzazione dei dati: art. 5, par. 1, lett. c), del GDPR).

La funzionalità di zoom dovrà essere utilizzata solo se indispensabile per verificare la effettiva sussistenza di un evento anomalo o se la ripresa ordinaria fosse resa inefficace dalle condizioni ambientali (luce, eventi atmosferici, presenza di ostacoli).

5.1.2. – Trattamento delle registrazioni

Devono svolgersi all'interno del complesso dell'Ente, in locali dove non vi sia afflusso di persone estranee alla Camera di commercio, le seguenti operazioni di trattamento:

1. registrazione delle immagini;
2. visione del registrato;
3. estrapolazione/scarico delle immagini dal sistema di registrazione;
4. realizzazione di eventuali copie di sicurezza;
5. consegna delle copie ai soggetti autorizzati.

Il trattamento è svolto mediante personale opportunamente istruito e previamente incaricato.

5.1.3. – Accesso ai locali da parte di soggetti diversi dagli incaricati

Eventuali accessi fisici ai locali dove si svolge il trattamento o dove sono collocati i registratori digitali da parte di persone diverse da quelle sopra indicate, devono essere autorizzati per iscritto, dal Titolare a meno che non si tratti di accessi necessari per le manutenzioni degli impianti relativi alla rete informatica, elettrici e di raffrescamento dei locali, fermo restando l'impossibilità dei manutentori di accedere fisicamente al DVR di registrazione delle immagini.

L'autorizzazione deve riportare:

- identificativo dell'autorizzato;
- lo scopo dell'accesso (breve descrizione dell'attività autorizzata);
- se possibile: la durata dell'accesso (orario di entrata e di uscita dai locali) oppure la stima del tempo necessario per lo svolgimento dell'attività autorizzata.

L'autorizzazione viene comunicata agli incaricati del trattamento interni o esterni, i quali dovranno accertarsi dell'identità della persona autorizzata prima di consentirne l'accesso ai locali dove si svolge il trattamento.

5.1.4. – Modalità di conservazione dei dati registrati

Secondo il sistema, le immagini possono essere memorizzate:

1. all'interno del dispositivo di registrazione;
2. in supporti esterni ed asportabili.

Le copie di immagini (realizzate secondo la procedura di accesso prevista dal successivo paragrafo 5.4.), sono conservate solo per il tempo intercorrente tra la loro realizzazione e la consegna materiale al richiedente.

Il supporto deve essere etichettato (o contrassegnato) indicando:

- l'identificativo del richiedente (nome dell'Autorità o del pubblico ufficiale o dell'avvocato);
- la data della richiesta;
- la data e l'orario delle riprese originali.

Vanno evitati riferimenti che consentano di identificare direttamente gli interessati, o di collegarli esplicitamente ad eventuali illeciti, presunti o contestati.

I supporti etichettati devono essere riposti in un armadio (o simili, per es. cassaforte) dotato di serratura, accessibile solo da parte dagli incaricati del trattamento. Il contenitore delle copie deve essere comunque ubicato in area ad accesso ristretto e controllato.

Le copie potranno essere consegnate soltanto all'Autorità o ai soggetti autorizzati che ne abbiano fatto richiesta. Le copie non ritirate devono essere distrutte secondo la procedura prevista dal successivo punto 5.1.6.

5.1.5. – Cancellazione dei dati registrati

Le immagini sono registrate con impianto digitale. Il sistema deve essere impostato in modo da cancellarle automaticamente e definitivamente secondo la tempistica stabilita e, comunque, entro i tempi di legge.

In caso di impossibilità di procedere automaticamente alla cancellazione, essa dovrà avvenire manualmente attraverso l'apposita funzionalità del registratore. Le operazioni dovranno essere effettuate nel locale dove è ubicato il registratore. Al loro termine l'operatore dovrà verificarne il risultato.

5.1.6. – Distruzione dei supporti esterni

Eventuali supporti contenenti copie realizzate su richiesta degli aventi diritto e non ritirati entro i tempi stabiliti, dovranno essere fisicamente distrutti in modo da renderne impossibile la ricostruzione ed il recupero dei dati.

Memorie di massa quali chiavette o hard disk, in caso di riutilizzo controllato, dovranno essere preventivamente sottoposte a formattazione di basso livello mediante apposito software, in modo da rendere impossibile il recupero dei dati memorizzati in precedenza.

Qualora destinate alla consegna a soggetti diversi dagli incaricati allo specifico ambito di trattamento, non dovranno essere riutilizzate ma essere anche smagnetizzate e distrutte.

5.2. – ACCESSO ALLE IMMAGINI TRATTATE

5.2.1. – Tipologie di accesso e relative modalità

Si prevedono i seguenti tipi di accesso, secondo le regole generali e specifiche, che costituiscono la procedura per l'accesso descritta nel prosieguo.

Tipo di accesso	Contenuto	Documentazione
-----------------	-----------	----------------

I) Acquisizione di copia delle registrazioni (ad uso esclusivo di Autorità o delle Forze dell'ordine, o avvocato nei casi previsti dalla legge)	Il richiedente è autorizzato o legittimato ad ottenere copia delle immagini registrate, riversate su di un supporto mobile. La ricerca delle immagini, la realizzazione delle copie e la loro consegna materiale avvengono a cura di un operatore autorizzato ed abilitato al trattamento.	✓ Richiesta dell'Autorità o delle Forze dell'ordine; ✓ Autorizzazione / richiesta del Titolare ✓ Autorizzazione al ritiro dei supporti da parte di persona identificata (in caso di impedimento del rappresentante del Titolare o del Responsabile interno); ✓ Compilazione del Verbale di consegna.
II) Accesso visivo	Il soggetto legittimato o autorizzato accede alla sola visione delle registrazioni, previa loro ricerca da parte di un operatore incaricato ed abilitato al trattamento.	✓ Richiesta dell'Autorità o delle Forze dell'ordine; ✓ Autorizzazione / richiesta del Titolare; ✓ Esercizio dei diritti dell'interessato a norma degli artt. 15 ss. del GDPR.

5.2.2. – Accertamento dell'esistenza di immagini trattate

Prima di dar corso a qualsiasi richiesta, il Titolare (o il suo delegato) accerterà l'effettiva esistenza delle immagini, avvalendosi degli operatori incaricati.

All'esito – attraverso i competenti uffici – darà formale e immediata comunicazione al richiedente dell'esito positivo o negativo dell'accertamento.

In caso di accertamento negativo, dovrà precisarne i motivi (per es. l'interessato non risulta ripreso; le immagini sono state cancellate entro i tempi di legge indicati nell'informativa, etc.).

5.2.3. – Registrazione degli accessi

Tutti gli accessi - comprese le richieste a cui si è dato riscontro negativo - devono essere registrati mediante l'annotazione di apposito registro, nel quale dovranno essere almeno riportati:

- Il tipo di accesso autorizzato (accesso visivo, rilascio di copie);
- la data e l'ora dell'accesso;
- l'identificazione del terzo autorizzato;
- gli estremi dell'autorizzazione all'accesso (data dell'autorizzazione e organo dell'Ente che ne ha concesso il rilascio).

Per il Registro degli accessi si rinvia, più avanti, al paragrafo 6.1.

5.3. – ACCESSO VISIVO

5.3.1. – Soggetti e personale abilitato all'accesso ai dati

L'accesso visivo alle immagini è consentito solo a:

Soggetto	Attività
Titolare del trattamento	Autorizza l'accesso. Tramite gli uffici competenti, presiede alla verifica ed alla tenuta (Compilazione e conservazione) del Registro degli Accessi.

Autorizzato al trattamento con specifico profilo di autorizzazione	Trasmette al Titolare o al Responsabile esterno / Delegato del Titolare le richieste di accesso. Ricerca le immagini e presenza agli accessi. Accede alle immagini in quanto necessario alle operazioni di trattamento.
--	---

5.3.2. – Terzi autorizzati all'accesso

Accedono visivamente alle immagini registrate:

Soggetto	Motivazione e legittimazione
Autorità Giudiziaria o le Forze dell'Ordine, o avvocato nei casi previsti dalla legge	Per indagini in corso, tutela di un diritto in giudizio, attività di prevenzione e repressione di illeciti. La richiesta si fonda su ordine, provvedimento o richiesta formale. Le Forze dell'ordine possono ottenere copia delle immagini, così come l'avvocato nei casi previsti dalla legge.
Interessato (soggetto ripreso)	Di regola, ne è escluso. Accesso eccezionale autorizzato formalmente da Titolare, in caso di: 1. comprovata e documentata necessità o di pericolo concreto e imminente; 2. esercizio dei propri diritti previsti dagli artt. 15 ss. del GDPR.

5.3.3. – Accesso da parte di una autorità o delle forze dell'ordine

L'accesso visivo alle immagini su richiesta o ordine di una Autorità o delle Forze dell'ordine, è disposto dal Titolare del trattamento.

Al tal fine, l'Incaricato che riceve la richiesta deve immediatamente darne notizia al Titolare ed al proprio Responsabile diretto. L'Autorità dovrà essere immediatamente avvisata sui tempi di conservazione.

Oltre all'operatore incaricato di ricercare le immagini, all'accesso dovrà essere presente un delegato del Titolare (i.e.: Segretario Generale) o un Incaricato del trattamento a ciò autorizzato...

Se formalmente richiesto, potrà essere realizzata una copia delle immagini al fine di consentire l'accesso oltre detto termine.

Il Titolare, tenuto conto delle esigenze istruttorie e dei motivi dell'accesso, fisserà il giorno, l'ora ed il luogo in cui il richiedente potrà visionare le immagini.

Qualora l'Autorità non richieda la consegna della copia delle immagini registrate, essa dovrà essere distrutta ad accesso ultimato.

5.3.4. – Accesso visivo da parte dell'interessato (soggetto ripreso)

Di regola, agli interessati (soggetti ripresi) non è consentito accedere, nemmeno visivamente, alle registrazioni. Pertanto, l'accesso visivo deve considerarsi eccezionale e motivato da circostanze gravi, oggettive e supportate da idonea dimostrazione di tali circostanze.

L'interessato può chiedere al Titolare di essere autorizzato all'accesso visivo alle immagini ex art. 15 del GDPR. La richiesta dovrà essere presentata secondo quanto previsto dalla procedura di cui ai successivi punti 5.4.3. e 5.4.4., e dovrà indicare i motivi che rendono indispensabile l'accesso, allegandone adeguata documentazione se disponibile o necessaria in relazione ai motivi della richiesta.

La ricerca delle immagini è riservata agli Incaricati, che applicano la procedura di cui al successivo punto 5.4.5.

Nel caso di accertamento positivo, il Titolare potrà disporre la conservazione temporanea di copia delle immagini e fisserà il giorno - non oltre 4 giorni dalla rilevazione - l'ora ed il luogo in cui il richiedente potrà visionare le immagini che lo riguardano direttamente, inviando all'interessato tempestiva comunicazione.

Le copie realizzate temporaneamente per consentire all'interessato l'accesso, a norma dell'art. 15, del GDPR, vanno conservate fino alla data di accesso visivo.

Una volta esercitato il diritto di accesso, in mancanza di una diversa disposizione da parte di una Autorità (per es. ordine di acquisizione), le immagini dovranno essere cancellate o i supporti distrutti.

5.3.5. – Conservazione dei dati registrati su richiesta dell'interessato (soggetto ripreso)

Qualora l'interessato, in veste di soggetto ripreso, ritenga di avvalersi di immagini per tutelare o esercitare un proprio diritto in giudizio, potrà richiedere la conservazione temporanea di eventuali registrazioni che lo riguardano. A tal fine, dovrà rivolgersi alle Autorità competenti, le quali ordineranno l'acquisizione delle registrazioni e/o la conservazione per un periodo superiore a quello di legge.

L'interessato dovrà presentare al Titolare formale richiesta scritta e motivata. La richiesta dovrà essere presentata secondo quanto previsto dalla procedura di cui al successivo punto 5.4.3. e dovrà essere corredata da una copia di denuncia-querela, da cui risulti la richiesta di acquisizione delle immagini quali mezzi di prova.

Le operazioni di ricerca delle immagini sono riservate ai soggetti autorizzati al trattamento. All'interessato non devono essere rilasciate copie delle immagini registrate.

5.3.6. – Esercizio dei diritti da parte dell'interessato (soggetto ripreso) ex artt. 15-22 del GDPR

L'interessato, in quanto soggetto ripreso, può fare istanza:

1. al Titolare del trattamento, rivolgendosi ai contatti della Camera di commercio individuati nell'informativa di cui all'art. 13 GDPR;
2. al Responsabile designato dal Titolare, ex art. 28 del GDPR, indicato nella suddetta informativa ;
3. al Responsabile della protezione dei dati (DPO) designato, indicato nella suddetta informativa.

L'eventuale esercizio dei diritti è condizionato dal preventivo accertamento dell'esistenza o meno di registrazioni che lo riguardano direttamente. A tal fine, il richiedente deve essere informato sui i tempi di conservazione delle immagini. Qualora la richiesta fosse soltanto verbale, il richiedente deve essere gentilmente invitato a compilare il modulo messo a disposizione dal Titolare o dal Responsabile designato.

Per facilitare il reperimento delle immagini di possibile interesse, l'istanza deve indicare:

- a quale impianto di videosorveglianza si fa riferimento;
- il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa;
- indicazioni sull'abbigliamento indossato, accessori ed altri elementi utili alla individuazione;
- presenza di altre persone;
- attività svolta durante le riprese.

Nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, deve essere data immediata comunicazione al richiedente degli elementi mancanti, in modo che egli possa integrare la richiesta.

Non possono essere accettate istanze presentate da persone diverse dal soggetto ripreso, fatti salvi i casi previsti dalla legge. A tal fine, il richiedente dovrà esibire un documento di identità in corso di validità i cui estremi dovranno essere registrati dall'incaricato, senza fare copia del documento stesso, da allegare alla richiesta. In caso di istanza pervenuta a mezzo fax e posta (tradizionale o cartacea), si darà corso alla richiesta solo se corredata da copia di un documento di identità valido.

L'allegazione del documento non è necessaria se l'interessato abbia sottoscritto la richiesta con la firma digitale, ovvero sia stato riconosciuto con altri sistemi di identità digitale (CNS, SPID, CIE).

5.4. – REALIZZAZIONE E CONSEGNA DI COPIE

5.4.1. – Personale autorizzato

Possono accedere alle registrazioni ed alle copie, in quanto necessario alle operazioni di trattamento:

Soggetto	Attività
Titolare del trattamento	Autorizza la conservazione delle registrazioni ed il rilascio delle copie. Accede al contenuto delle copie in quanto necessario all'individuazione delle immagini richieste ed al controllo dello stato dei supporti.
Autorizzato al trattamento con specifico profilo di autorizzazione	Trasmette le richieste al Titolare o ai suoi delegati. Ricerca le immagini e ne realizza le copie. Accede al contenuto delle copie in quanto necessario all'individuazione delle immagini richieste ed al controllo dello stato dei supporti. Custodisce i supporti e ne cura la consegna.

5.4.2. – Soggetti terzi autorizzati ad ottenere copia delle registrazioni

L'accesso tramite acquisizione di copia delle registrazioni è riservato:

1. all'Autorità Giudiziaria o alle Forze dell'Ordine, dietro loro ordine (per es. provvedimento giudiziario, verbale, etc.) o previa loro formale richiesta, scritta e motivata. A tal fine, ricorrendone i presupposti di legge (per es. indagini in corso, tutela in giudizio di un diritto, attività di prevenzione del crimine o di un pericolo imminente, etc.) l'Autorità può ordinare un prolungamento dei tempi di conservazione delle immagini;
2. agli altri soggetti pubblici e privati, nei casi previsti dalla legge;
3. al Titolare, previa formale richiesta scritta. Nel caso di un loro impedimento, i supporti contenenti le registrazioni potranno essere consegnate a persone di loro fiducia, preventivamente individuate e autorizzate per iscritto. I nominativi dovranno essere trasmessi agli operatori incaricati unitamente alla richiesta delle copie.

Non è prevista la realizzazione, né la consegna di copie a soggetti diversi da quelli individuati al punto precedente.

5.4.3. – Forma e contenuto della richiesta

L'Autorità richiedente (o il diverso soggetto, nei casi previsti dalla legge) deve presentare apposita istanza scritta al Titolare, o al Responsabile del trattamento indicato nell'informativa.

Al fine di verificarne la provenienza, l'istanza deve essere redatta, alternativamente, su:

- carta intestata dell'Autorità (o soggetto) richiedente;
- su modulo del richiedente, contenente gli estremi identificativi dell'Autorità;
- su modulo fornito dal Titolare o dal Responsabile.

In ogni caso, essa deve riportare la data di presentazione, la firma (o sigla) e gli estremi identificativi del pubblico ufficiale (o altro soggetto) richiedente.

Nel caso in cui il richiedente sia il Titolare , dovrà essere consegnata all'operatore incaricato apposita richiesta scritta, da cui risulti quale operazione di accesso egli deve compiere:

1. ricerca delle immagini;
2. visione del registrato;
3. estrapolazione / scarico delle immagini dal sistema di registrazione;
4. realizzazione di eventuali copie di sicurezza;
5. consegna delle copie a soggetti identificati ed autorizzati.

Oltre agli elementi utili per facilitare il reperimento delle immagini di possibile interesse (per es. impianto di videosorveglianza di riferimento, data e ora in cui sono state effettuate le riprese di possibile interesse), l'istanza deve indicare le motivazioni per cui viene chiesta copia delle registrazioni (per es. indagini nell'ambito di un procedimento in corso avanti l'Autorità giudiziaria, etc.).

Nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data immediata comunicazione al richiedente, invitandolo alle necessarie integrazioni.

5.4.4. – Modalità di presentazione della richiesta

In caso di istanza su modulo dell'Autorità, essa deve essere presentata con modalità tali da garantire la certezza del mittente (Fax, PEC, Racc. A/R, etc.). Qualora sia presentata oralmente da un pubblico ufficiale, quest'ultimo deve essere adeguatamente informato e invitato a presentare richiesta scritta, avvalendosi eventualmente della modulistica a disposizione.

All'atto della presentazione dell'istanza, il richiedente deve essere informato circa i tempi di conservazione delle immagini. Nel caso in cui le immagini di possibile interesse non risultino conservate o siano state già cancellate ne dovrà essere data immediata comunicazione al richiedente.

Qualora l'istanza venga direttamente presentata all'operatore autorizzato al trattamento, questi deve inoltrarla immediatamente al Titolare , che avviserà il Responsabile per la protezione dei dati (RPD). L'Incaricato deve avvisare il proprio Responsabile di riferimento.

5.4.5. – Ricerca delle immagini e riproduzione in copia

Il Titolare – sulla base degli elementi contenuti nella richiesta - accerterà l'effettiva esistenza delle immagini, attivando tramite comunicazione scritta gli operatori incaricati con il necessario profilo di autorizzazione.

Gli operatori procederanno alla ricerca delle immagini, comunicandone l'esito al Titolare.

Il Titolare dà comunicazione al richiedente (Autorità o Forze dell'Ordine, o altro soggetto legittimato nei casi previsti dalla legge) dell'esito positivo o negativo dell'accertamento.

In caso di:

- a. accertamento negativo, dovranno essere precisati i motivi (per es. l'interessato non risulta ripreso; le immagini sono state cancellate entro i tempi di legge indicati nell'informativa, etc.);
- b. accertamento positivo, dovranno essere comunicati al richiedente il giorno, l'ora ed il luogo in cui potranno essere prelevate le copie richieste.

Se durante la ricerca dovessero essere rilevate immagini:

- di fatti che integrano ipotesi di reato o altri eventi rilevanti ai fini dell'intervento delle forze dell'ordine;
- di qualsiasi altra situazione anomala afferente ai visitatori, dipendenti od al patrimonio.

L'Incaricato informerà immediatamente il Titolare ed il proprio Responsabile diretto, attendendo istruzioni.

5.4.6. – Realizzazione e consegna di copie

Su formale richiesta del Titolare o del Responsabile designato, gli operatori incaricati riverseranno sul supporto esterno le immagini da conservare. Il supporto dovrà essere etichettato e conservato, secondo quanto previsto al precedente punto 5.1.4.

I supporti contenenti immagini registrate non devono mai essere asportati dai locali dell'Ente in cui sono collocati. La consegna di eventuali copie richieste da una Autorità (o altro soggetto legittimato) avviene presso i locali individuati dal Titolare.

Al momento della consegna materiale al soggetto legittimato, dovrà essere redatto un apposito verbale, in cui dovranno essere indicati:

- riferimento alle immagini duplicate, come da etichettatura del supporto (per es. riprese in data XYZ, riferite a presunto illecito avvenuto in ABC);
- data e ora della consegna del supporto;
- tipo del supporto (CD, DVD, chiavetta USB, hard disk, etc.);
- identificativo e firma (o sigla) della persona o dell'ufficio che ha curato la consegna;
- identificativo e firma (o sigla) del ricevente (Ufficio del Titolare, pubblico ufficiale che ha curato il ritiro dei supporti).

Le copie realizzate su ordine dell'Autorità vanno conservate fino al momento del loro prelievo da parte del pubblico ufficiale incaricato dalla richiedente.

Qualora le immagini non fossero acquisite dall'Autorità entro il termine indicato dall'autorità stessa per il ritiro (o non fosse stata indicata alcuna scadenza), gli operatori incaricati ne daranno notizia al Titolare, che contatterà l'Autorità richiedente prima di disporre la eventuale cancellazione o distruzione dei supporti.

6 - PARTE V – REGISTRO ATTIVITA' DI VIDEOSORVEGLIANZA

6.1.– REGISTRO DELLE ATTIVITA' DI VIDEOSORVEGLIANZA

È istituito il Registro delle attività di videosorveglianza, costituito dai seguenti due Registri (o Sezioni):

- a) Registro dei Soggetti autorizzati al trattamento per la Videosorveglianza;
- b) Registro degli accessi e delle richieste di copie di dati della Videosorveglianza

I modelli per i relativi Registri sono riportati negli Allegati 8 e 9.

Il Registro delle attività di videosorveglianza è tenuto da soggetti all'uopo incaricati dalla Camera di commercio che ne cura la compilazione, la verifica e l'archiviazione.

7 - PARTE VI – ELENCO DEGLI ALLEGATI

7.1. – ALLEGATI

Costituiscono Allegati al presente Disciplinare i seguenti:

Allegato 1 - Nomina del Responsabile esterno per la Videosorveglianza, ex art.28 del GDPR;

Allegato 2- Modello di cartello/informativa breve sulla Videosorveglianza;

Allegato 3 - Modello di Informativa estesa sulla Videosorveglianza, ex art. 13 del GDPR

Allegato 4 - Modulo per Accesso del Titolare o di un suo delegato ai dati della Videosorveglianza;

Allegato 5 - Modulo per l'accesso delle Autorità o delle Forze dell'ordine a dati/immagini della Videosorveglianza;

Allegato 6 - Modulo per l'esercizio dei diritti dell'interessato ai dati/immagini della Videosorveglianza;

Allegato 7 - Modello di verbale per la consegna di immagini da Videosorveglianza;

Allegato 8 – Classificazione dei soggetti autorizzati e Modello di Registro dei soggetti autorizzati al trattamento per la Videosorveglianza;

Allegato 9 - Modello di Registro degli accessi e delle richieste di copie di dati della Videosorveglianza.

Spett.le

.....

Oggetto: *Nomina a Responsabile esterno del trattamento di dati personali, ai sensi degli articoli 4, co. 8 e 28 del Regolamento UE n. 679/2016.*
RIF. contratto _____

Il sottoscritto _____, in qualità di Segretario Generale della Camera di commercio, industria, artigianato e agricoltura di _____ (di seguito anche "Camera di commercio" o "Titolare") e soggetto che, secondo gli ordinari criteri di imputazione della volontà dell'Ente, è deputato in relazione al rapporto in oggetto ad esternare la volontà del Titolare del trattamento.

PREMESSO CHE

- ai sensi dell'art. 4, n. 7), del Regolamento UE n. 679/2016 (di seguito "GDPR"), la Camera di commercio è Titolare dei trattamenti sui dati personali che effettua per lo svolgimento delle proprie funzioni istituzionali, in quanto determina le decisioni in ordine alle finalità ed ai mezzi dei trattamenti (anche affidati all'esterno);
- la (*Indicare i dati del Responsabile*) _____ (di seguito anche _____) è risultata aggiudicataria di una procedura aperta per l'affidamento del servizio di vigilanza e video sorveglianza della sede della Camera di commercio che prevede i seguenti servizi (*precisare e/o adattare all'oggetto quanto riportato nel box seguente*):

- Vigilanza fissa;
- Televigilanza e videosorveglianza attraverso collegamenti complessi ad alto contenuto tecnologico;
- Fornitura, posa, installazione e manutenzione di un impianto di videosorveglianza in aggiunta ed integrazione ai sistemi di videosorveglianza esistenti;
- Altro ...

- Le attività oggetto dell'incarico comportano il trattamento delle seguenti tipologie di dati personali:

1.;
2.;
3.

Si fa presente, al riguardo, che la videosorveglianza NON può riguardare il controllo delle prestazioni lavorative dei dipendenti della Camera di commercio.

- la verifica del possesso dei requisiti di esperienza, capacità ed affidabilità finalizzate a fornire "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato" richiesta dall'art. 28, par. 1 del GDPR, è stata effettuata dalla scrivente Camera di commercio nell'ambito dell'espletamento della procedura ad evidenza pubblica innanzi citata; in particolare, le misure di sicurezza tecniche, informatiche ed organizzative poste in essere sono state valutate come idonee, in relazione alla natura, oggetto, contesto e finalità del trattamento come definito

nell'incarico di cui in oggetto. La Camera di commercio si riserva, comunque, a sua discrezione, una verifica, qualora gli impianti del trattamento non siano nella disponibilità della Camera di commercio, anche mediante apposito audit, con particolare riferimento alla loro adeguatezza e ai trattamenti effettuati per suo conto;

- nell'ambito della stessa procedura, la Camera di commercio ha provveduto ad autorizzare _____, anche ai fini del par. 2 del citato art. 28 del GDPR, ad avvalersi della Società _____ (*Precisare se il Responsabile può avvalersi di altri soggetti che eventualmente già operano per conto dell'Ente*) cui sono state affidate attività di configurazione e manutenzione degli impianti, dei profili utenti, del sistema di conservazione e cancellazione dei dati, nonché l'adozione di ulteriori misure di sicurezza logiche a protezione dei dati;
- ai sensi dell'articolo 28 del GDPR, l'affidamento di un trattamento di dati ad un Responsabile esterno deve essere regolato da un contratto o da analogo atto giuridico che vincoli i due soggetti e ne definisce le reciproche responsabilità e comprenda, fra l'altro le istruzioni del Titolare (la Camera di commercio) impartite al Responsabile;
- il Provvedimento del Garante per la protezione dei dati personali "*Provvedimento in materia di videosorveglianza*" dell'8 aprile 2010, pubblicato in G.U. n. 99 del 29 aprile 2010 prescrive adempimenti specifici in relazione alla raccolta, registrazione, conservazione e, in generale, utilizzo di immagini attraverso sistemi di videosorveglianza;
- le prescrizioni contenute in detto Provvedimento vanno aggiornate con le più recenti indicazioni contenute nelle Linee guida 3/2019 del Comitato europeo per la protezione dei dati (EDPB), sul trattamento dei dati personali attraverso dispositivi video, versione 2.0, adottate il 29 gennaio 2020;
- trovano applicazione le disposizioni contenute nell'apposito Disciplinare per i trattamenti relativi alla videosorveglianza, adottato dalla Camera di commercio (nel prosieguo "Disciplinare");
- con la sottoscrizione del presente atto, la Società in qualità di Responsabile esterno del trattamento ex art. 28 del GDPR, - accetta la suddetta nomina confermando la diretta ed approfondita conoscenza degli obblighi che si assume e assicura, sotto la propria responsabilità, di aver adempiuto o di adempiere, in funzione delle caratteristiche del trattamento affidato, alle seguenti istruzioni; in proposito, la Camera di commercio potrà, a sua completa discrezione ove ritenuto necessario, richiedere al soggetto sopra menzionato una dimostrazione documentale sull'osservanza delle disposizioni impartite, anche mediante una ispezione;
- la sottoscrizione per accettazione della presente lettera di nomina costituisce condizione di efficacia ed esecutività dell'incarico citato in oggetto.
- tutto ciò premesso, da considerarsi parte integrante e sostanziale del presente atto,

ISTRUZIONI IMPARTITE AL RESPONSABILE

L'attività oggetto di affidamento comporta per il Responsabile che opera per conto del Titolare, il trattamento di dati personali ed in particolare di immagini, con possibilità di identificazione dei soggetti ripresi (dipendenti, collaboratori e visitatori della Camera di commercio).

Le immagini sono acquisite, visualizzate e conservate e quindi possono essere trattate, in conformità a quanto definito contrattualmente, al solo fine di garantire la sicurezza del patrimonio aziendale e per la rilevazione di eventuali situazioni di pericolo. La misura è complementare e non sostitutiva rispetto all'attività dell'Autorità Giudiziaria o delle Forze dell'Ordine.

La durata dell'incarico del trattamento è definita con rinvio alla durata del contratto. I termini di conservazione dei dati personali della videosorveglianza e tutta la relativa regolamentazione è contenuta nel Disciplinare citato in premessa, al quale si rinvia.

Il Responsabile _____ si impegna espressamente:

- a) a comunicare prontamente alla Camera di commercio – indirizzando le comunicazioni presso la pec istituzionale dell'Ente, di cui in calce, eventuali situazioni sopravvenute (tra cui a puro titolo esemplificativo, sanzioni comminate dall'Autorità Garante o da Autorità Giudiziarie ordinarie, anche non relative alle attività di trattamento oggetto del presente atto) che, per qualsiasi ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico;
- b) a non utilizzare i dati personali acquisiti per finalità che non siano strettamente attinenti al contratto di cui in oggetto;
- c) ad individuare ed autorizzare i soggetti (persone fisiche), debitamente formati, che per suo conto svolgeranno il trattamento, impartendo loro adeguate e documentate istruzioni al fine di garantire il rispetto della normativa precedentemente richiamata, delle condizioni di liceità del trattamento e dei vincoli impartiti attraverso il presente atto, nonché ad ottenere da questi un formale impegno alla riservatezza. Le prescrizioni contenute nel Disciplinare costituiscono parte integrante delle istruzioni da conoscere;
- d) ove il contratto di cui in oggetto non preveda una autorizzazione generale in proposito, a non ricorrere ad eventuali ulteriori sub-contrattanti senza previa autorizzazione scritta da parte della Camera di commercio; l'autorizzazione potrà essere eventualmente rilasciata sulla base di una preventiva verifica di affidabilità di tali soggetti condotta e rendicontata dal Responsabile al Titolare, finalizzata a garantire lo stesso livello di sicurezza nei trattamenti; in caso di autorizzazione, il Responsabile dovrà adottare opportune clausole contrattuali al fine di richiamare in capo ai sub-contrattanti l'obbligo di rispettare le misure e gli accorgimenti stabiliti dalla presente designazione nonché un analogo livello di sicurezza adottato dal contraente e valutato come idoneo dalla Camera di commercio. Le stesse modalità sono valide anche per le eventuali aggiunte o sostituzione dei sub-responsabili **ovvero** nell'eventualità di successivo affidamento a terzi (persone fisiche/giuridiche individuate come sub-responsabili esterni del trattamento, con l'esclusione che questi ultimi possano, a loro volta, nominare propri sub-responsabili) di parte delle attività previste, la Società si impegna, altresì:
 - a verificare preventivamente l'affidabilità di tali soggetti al fine di garantire al Titolare lo stesso livello di sicurezza nei trattamenti;
 - ad adottare opportune clausole contrattuali al fine di richiamare in capo ai medesimi soggetti l'obbligo di rispettare le misure e gli accorgimenti stabiliti;
- e) per effetto dell'autorizzazione all'utilizzo dei sub-responsabili individuati, ad imporre contrattualmente e ad accertarsi che il sub-responsabile provveda:
 - alla designazione individuale degli Amministratori di sistema (o figura equivalente), secondo le prescrizioni del Garante privacy, coinvolti nelle attività di cui in oggetto, previa valutazione delle caratteristiche di esperienza, capacità, e affidabilità, anche in considerazione delle responsabilità che possono derivare in caso di incauta o inadeguata designazione;
 - a riportare, per ciascuna figura coinvolta, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
 - a verificare periodicamente – anche attraverso idonei sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici, che dovranno essere conservati per almeno sei mesi a far data dalla conclusione delle attività contrattuali - l'operato di tali figure in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza adottate;In proposito, il Responsabile si impegna inoltre:
 - ad acquisire ed a fornire alla Camera di commercio, a semplice richiesta e secondo le modalità indicate da quest'ultima, l'elenco degli Amministratori di sistema o figure equivalenti designate dal sub-responsabile, nonché l'esito delle valutazioni sull'operato di tali figure;
 - a comunicare alla Camera di commercio, prima dell'inizio delle relative attività, il nominativo di eventuali ulteriori soggetti coinvolti nei trattamenti nonché tutti gli ulteriori elementi utili affinché il Titolare possa autorizzare od opporsi espressamente al loro coinvolgimento;
- f) ad adottare procedure di controllo sull'attività svolta dai soggetti di cui ai punti c), d) ed e), al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate, degli obblighi di riservatezza e, comunque, delle istruzioni impartite;
- g) a non comunicare comunque ad ulteriori soggetti terzi i dati oggetto di trattamento, senza preventiva autorizzazione scritta della Camera di commercio;

- h) ad adottare tutte le misure di sicurezza tecnico-informatiche ed organizzativo-gestionali dichiarate in fase contrattuale ed esplicitate nel Disciplinare adottato dalla Camera di commercio; nell'eventualità di modifica delle stesse (ad es., in caso di modifiche evolutive di infrastrutture, apparati, applicativi di lavoro e modalità gestionali) dovrà essere garantito – ad esito di specifica analisi di impatto – un livello di sicurezza almeno analogo a quello risultante dall'analisi dei rischi formalizzata; in caso contrario, è fatto specifico obbligo di condividere con il referente contrattuale della Camera di commercio le nuove specifiche di trattamento, al fine di consentire la verifica del mantenimento dell'idoneità allo svolgimento dell'incarico;
- i) a provvedere, nei confronti degli interessati che si rivolgessero direttamente a propri soggetti coinvolti nei trattamenti, al rilascio dell'informativa concordata con la Camera di commercio e riportata in allegato al citato Disciplinare;
- j) a garantire tempestivamente idoneo riscontro all'interessato in caso di richiesta diretta di esercizio dei diritti di cui agli artt. 15 e ss., del GDPR, informando contestualmente la Camera di commercio in tutti i casi in cui tale attività possa risultare dannosa ai fini della corretta esecuzione dell'incarico o possa comportare un qualsivoglia pregiudizio all'Ente stesso (ad es., richiesta di blocco o limitazione del trattamento);
- k) a fornire alla Camera di commercio, a semplice richiesta e secondo le modalità indicate da quest'ultima, i dati e le informazioni necessarie per:
 - una tempestiva difesa in eventuali procedure instaurate davanti all'Autorità garante o Giudiziarie per effetto del trattamento dei dati in cui sia coinvolto il Responsabile;
 - dare tempestivo riscontro all'interessato che eserciti i diritti di cui al punto precedente direttamente nei confronti della Camera di commercio;
 - compiere tempestivamente quanto necessario per conformarsi a richieste pervenute dal Garante o dall'Autorità giudiziaria o, comunque, dalle Forze dell'Ordine.

Il Responsabile si impegna inoltre espressamente:

- l) a comunicare eventuali violazioni dei dati personali o presunte tali (a puro titolo esemplificativo: accessi abusivi, azione di malware, incendi o altre calamità, etc.) che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse, al fine di consentire alla Camera di commercio, se del caso, l'adempimento degli obblighi di notificazione al Garante ed agli interessati, come previsto dagli artt. 33 e 34 del GDPR. La comunicazione deve avvenire **entro 24 ore** dal momento in cui la Società ... è venuta a conoscenza della violazione con l'obbligo di collaborare attivamente con la Camera di commercio, con i suoi delegati e con il Responsabile per la Protezione dei Dati (RPD/DPO), nella raccolta documentale e in tutte le attività connesse all'eventuale notifica al Garante e ai soggetti interessati, per quanto previsto nella normativa vigente;
- m) a fornire, in caso di necessità, la massima disponibilità e collaborazione affinché il Titolare possa, direttamente o per il tramite di consulenti di propria fiducia, condurre verifiche anche presso la sede della Società ... e degli altri Sub-responsabili eventualmente designati;
- n) a prestare, in generale, la più ampia e completa collaborazione alla Camera di commercio e al suo RPD/DPO, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- o) in fase di rendicontazione delle attività svolte, a relazionare alla Camera di commercio sul buon esito delle attività di trattamento secondo gli standard precedentemente definiti, confermando esplicitamente l'assenza di qualsivoglia copia delle registrazioni autonomamente effettuate o conservate.

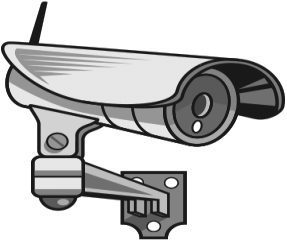
Ai sensi e per gli effetti delle istruzioni impartite, il Responsabile per l'esecuzione del contratto di cui la presente nomina è parte è il Dr./D.ssa _____ che agisce anche in qualità di Sostituto delegato dal Titolare ed a cui fare riferimento per qualsivoglia problematica o comunicazione inerente il presente incarico.

INOSSERVANZA DELLE ISTRUZIONI E RISOLUZIONE

1. Fatte salve le disposizioni del GDPR e del Codice della privacy, qualora il Responsabile violi gli obblighi che gli incombono a norma della presente nomina, la Camera di commercio può dare istruzioni per sospendere il trattamento dei dati personali fino a quando il Responsabile rispetti le presenti istruzioni o non sia risolto il contratto.
2. Il Responsabile informa prontamente la Camera di commercio qualora, per qualunque motivo, non sia in grado di rispettare le istruzioni di cui alla presente nomina.
3. La Camera di commercio ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali qualora:
 - a) il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare del trattamento ai sensi del precedente punto 1 e il rispetto delle istruzioni di cui alla nomina non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
 - b) il Responsabile violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del GDPR o del Codice della privacy;
 - c) il Responsabile non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi sul trattamento dei dati personali.
4. Sono in ogni caso fatte salve le penalità, previste dal contratto indicato in oggetto, con riferimento al trattamento di dati personali, nonché l'obbligo - da parte del Responsabile - di tenere manlevato il Titolare qualora ricorrano le casistiche di cui al comma 3 sopra individuato
5. il Responsabile ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali sulla base delle istruzioni della presente nomina qualora - dopo aver informato la Camera di commercio che, a suo parere motivato, le istruzioni del Titolare violano il GDPR o le disposizioni applicabili, nazionali o comunitarie, relative alla protezione dei dati - la Camera di commercio insista sul rispetto delle istruzioni.
6. In caso di violazione delle disposizioni impartite, determinando autonomamente le finalità e i mezzi del trattamento, oltre alla comminazione delle sanzioni contrattualmente previste, il Responsabile risponderà per qualsiasi danno causato agli interessati.

La presente nomina è valida per tutto il periodo di durata degli accordi contrattuali e dei successivi eventuali rinnovi. È da ritenere revocata, con effetto immediato e senza obbligo di preavviso, in caso di recesso unilaterale o consensuale dall'incarico citato in premessa.

Pregando di restituire alla Camera di commercio una copia della presente lettera, datata e firmata per accettazione, via **pec**, all'indirizzo, si inviano i più cordiali saluti.

	SISTEMA DI VIDEOSORVEGLIANZA INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI A NORMA DELL'ART.13 DEL REGOLAMENTO UE N. 679/2016 (GDPR)
TITOLARE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI	Titolare del trattamento è dei dati personali è la Camera di commercio, industria, artigianato e agricoltura di Reggio Calabria (di seguito "Camera di commercio") con sede in Via Tommaso Campanella, 12 contattabile per posta ordinaria, telefono o PEC ai seguenti recapiti: Tel.: 0965384111 PEC: cameradicommercio@rc.legalmail.camcom.it Presso la Camera di commercio opera il Responsabile della protezione dei dati (RPD), designato ai sensi dell'art. 37 del GDPR, contattabile ai seguenti recapiti: E-mail: dpo@rc.camcom.it.
FINALITÀ DEL TRATTAMENTO E BASE GIURIDICA	Per esigenze di sicurezza dei soggetti che transitano presso i locali dell'Ente e tutela del patrimonio della Camera di commercio (ovvero per scongiurare il rischio di furti, danneggiamenti, manomissioni), all'esterno e all'interno dell'Ente sono installate videocamere di sorveglianza che, inevitabilmente, raccolgono dati personali (immagini) di chiunque entri nel campo visivo delle telecamere stesse. Il presente cartello ne segnala l'esistenza in prossimità del perimetro di ripresa. Base giuridica del trattamento è il perseguimento del legittimo interesse del Titolare (a norma dell'art. 6, par. 1, lettera f), del GDPR), per le finalità sopra indicate. I dati personali trattati: a) non sono diffusi in alcuna forma; b) sono comunicati unicamente agli aventi diritto nei casi previsti dalla legge; c) non sono soggetti ad alcun processo decisionale automatizzato, compresa la profilazione.
RESPONSABILI DEL TRATTAMENTO	La Camera di commercio ha nominato, ex art. 28 del GDPR, un Responsabile del trattamento che si occupa della visione delle immagini della videosorveglianza. I relativi dettagli possono essere richiesti al Responsabile per la protezione dei dati (dpo@rc.camcom.it).
PERIODO DI CONSERVAZIONE	Le immagini registrate sono conservate, di regola, per 24 ore, , nonché nei casi in cui pervengano specifiche richieste in tal senso dalle Forze dell'Ordine, dall'Autorità Giudiziaria o da altri soggetti legittimati, a norma di legge, a farlo. Decorsi tali termini, le immagini sono automaticamente cancellate.
I DIRITTI DELL'INTERESSATO	L'interessato al trattamento può rivolgersi al Titolare o al RPD (contattabili ai recapiti sopra indicati) per esercitare, fra l'altro, i diritti di accesso e cancellazione previsti dal GDPR.
INFORMATIVA COMPLETA	L'informativa completa sul trattamento dei dati è disponibile presso i locali del Titolare.

MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA

(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)

Per informazioni: www.garanteprivacy.it/faq/videosorveglianza



L'informativa completa sul trattamento dei dati è disponibile presso i locali del Titolare.

LA RIPRESA E REGISTRAZIONE DELLE IMMAGINI È EFFETTUATA DALLA **CAMERA DI COMMERCIO DI REGGIO CALABRIA**.
CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI:
DPO@RC.CAMCOM.IT

LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI **24 ORE**, SALVA LA CONSERVAZIONE A SEGUITO DI RICHIESTA DA PARTE DELL'AUTORITÀ GIUDIZIARIA O DI POLIZIA.

FINALITÀ DELLA VIDEOSORVEGLIANZA:
TUTELA DEI SOGGETTI CHE TRANSITANO PRESSO LA SEDE E DEL PATRIMONIO DEL TITOLARE.

È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI A **DPO@RC.CAMCOM.IT**

INFORMATIVA AI SENSI DELL'ART. 13 DEL REGOLAMENTO (UE) N. 679/2016, RELATIVA AI TRATTAMENTI DEI DATI PERSONALI EFFETTUATI DALLA CAMERA DI COMMERCIO NELL'AMBITO DELLE PROCEDURE DI VIDEOSORVEGLIANZA

La presente informativa fornisce agli interessati le informazioni, inerenti il trattamento di dati personali, effettuato dalla Camera di commercio, industria, artigianato e agricoltura di Reggio Calabria (di seguito indicata anche come "Camera di Commercio" o "Titolare") mediante procedure di videosorveglianza.

L'informativa è stata redatta secondo quanto previsto:

- a) dall'art. 13 del Regolamento (UE) n. 679/2016 ("GDPR");
- b) dalle Linee Guida n. 3/2019, del 29 gennaio 2020, del Comitato Europeo sulla Protezione dei Dati (EDPB) e dal provvedimento del Garante, dell'8 aprile 2010, in materia di videosorveglianza;
- c) dal Disciplinare sulla videosorveglianza della Camera di commercio di Reggio Calabria.

1. TITOLARE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Titolare del trattamento dei dati personali è la Camera di Commercio di Reggio Calabria con sede in via Tommaso Campanella n. 12 Tel 0965384111 PEC cameradicommercio@rc.legalmail.camcom.it

L'Ente ha nominato, ai sensi dell'art. 37 del GDPR, il Responsabile della Protezione dei Dati (RPD/DPO) che è contattabile alla seguente mail dpo@rc.camcom.it

2. FINALITÀ E BASE GIURIDICA DEI TRATTAMENTI

2.1 Finalità

I dati personali raccolti e trattati tramite gli impianti di videosorveglianza e i sistemi di videoregistrazione sono le immagini di persone che si trovano nel raggio di ripresa delle telecamere, secondo quanto segnalato anche dalle apposite informative brevi.

Tali immagini sono trattate esclusivamente al fine di garantire la sicurezza e l'incolumità del personale del Titolare e di tutti coloro che, a qualsiasi titolo legittimo, accedono alla sede e agli spazi di pertinenza della Camera di commercio, nonché allo scopo di tutelare il patrimonio della Camera di commercio prevenendo e perseguendo il compimento di eventuali atti illeciti.

Tali misure di tutela sono complementari e non sostitutive rispetto all'attività delle Forze dell'Ordine e dell'Autorità giudiziaria.

2.2 Base giuridica

L'attività di videosorveglianza è basata sul perseguimento del legittimo interesse da parte del Titolare, ai sensi dell'art. 6, par. 1, lett. f), del GDPR.

3. DATI TRATTATI E MODALITÀ DEL TRATTAMENTO

3.1 Categoria di dati trattati

I dati trattati sono immagini di persone e cose presenti nel raggio di ripresa delle videocamere, con possibilità di identificazione dei soggetti ripresi.

3.2 Modalità del trattamento

L'impianto di videosorveglianza è in funzione 24 ore su 24, 7 giorni su 7 ed è dotato di un adeguato numero di telecamere che inquadrano spazi di pertinenza dell'Ente o di accesso e uscita (cancelli, portoni, parcheggi, etc.) e di videoregistratori digitali adeguatamente dislocati e collegati con le videocamere, anche da remoto. Tali sistemi consentono la visione delle immagini in tempo reale e la registrazione delle stesse.

In caso di allarme, generato da un evento in corso, è possibile il collegamento dalla centrale di controllo.

ALL. 3 – INFORMATIVA ESTESA SULLA VIDEOSORVEGLIANZA

La visione delle immagini riprese in tempo reale e la gestione delle registrazioni effettuate attraverso gli impianti di videosorveglianza, compresa la facoltà di estrapolarle e realizzarne copie, sono riservate al Titolare e/o al Responsabile del trattamento e/o alle persone da questi formalmente incaricate. I dati sono conservati con l'impiego di misure di sicurezza, fisiche e logiche, idonee a impedire l'accesso da parte di personale non autorizzato e a garantire la riservatezza e l'integrità degli stessi.

Gli apparati sono regolarmente mantenuti da parte di personale specializzato con profili di Amministratore di Sistema, preventivamente individuato, formato ed istruito.

A seguito delle richieste di accesso ai dati da parte dell'interessato, dell'Autorità giudiziaria e/o dalle Forze dell'ordine o di altri soggetti legittimati, Il trattamento complementare ed accessorio delle informazioni relative alle immagini avviene con strumenti elettronici e cartacei.

4. SOGGETTI AUTORIZZATI AL TRATTAMENTO

Il trattamento viene svolto da personale appartenente alla struttura del Titolare o del Responsabile del trattamento che opera per conto del Titolare, appositamente autorizzato, previamente e debitamente formato ed istruito per trattare i dati a norma di legge.

Il Titolare ha designato a norma dell'art. 28 del GDPR un Responsabile del trattamento per la gestione del servizio di videosorveglianza, i cui dettagli possono essere richiesti al Titolare del trattamento.

5. AMBITO DI COMUNICAZIONE E DIFFUSIONE DEI DATI

Oltre che ai soggetti interni autorizzati al trattamento, i dati potranno essere comunicati a soggetti pubblici e privati legittimati, nei casi previsti dalla legge, a richiedere i dati, come l'Autorità giudiziaria e/o di pubblica sicurezza.

Le immagini non sono soggette a diffusione né saranno trasferite in Paesi non appartenenti all'Unione europea, ovvero ad Organizzazioni internazionali.

6. PERIODO DI CONSERVAZIONE DELLE EVENTUALI REGISTRAZIONI

Le immagini contenute nelle videoregistrazioni sono conservate, di regola, per un massimo di 24 ore dalla rilevazione, fatto salvo il caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità giudiziaria, degli Organi di polizia o dell'interessato o di altri soggetti nei casi previsti dalla legge. Decorso tale termine, le immagini sono automaticamente cancellate e non più recuperabili.

I dati sono conservati presso il Titolare o il Responsabile del trattamento, in locali ad accesso ristretto e controllato.

7. ASSENZA DI UN PROCESSO DECISIONALE AUTOMATIZZATO

La Camera di commercio non adotta alcun processo automatizzato, compresa la profilazione, di cui all'art. 22, parr. 1 e 4, del GDPR, impiegando a questo scopo immagini dell'interessato.

8. DIRITTI DELL'INTERESSATO, LIMITI E MODALITÀ DEL LORO ESERCIZIO

8.1 Diritti dell'interessato

All'interessato – ex art. 13 - è garantito l'esercizio dei diritti riconosciuti dagli artt. 15 ss. del GDPR.

In particolare, è garantito, secondo le modalità e nei limiti previsti dalla vigente normativa, nonché di quanto indicato al successivo punto 8.2, l'esercizio dei seguenti diritti:

- richiedere la conferma dell'esistenza di dati personali che lo riguardino;
- conoscere la fonte e l'origine dei propri dati;
- riceverne comunicazione intelligibile;
- ricevere informazioni circa la logica, le modalità e le finalità del trattamento;
- richiedere l'aggiornamento, la rettifica, l'integrazione, la cancellazione e/o la limitazione dei dati

ALL. 3 – INFORMATIVA ESTESA SULLA VIDEOSORVEGLIANZA

trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti;

- opporsi al trattamento, per motivi connessi alla propria situazione particolare;
- revocare il consenso, ove previsto come base giuridica del trattamento. La revoca non pregiudica la legittimità del trattamento precedentemente effettuato;
- nei casi di trattamento basato sul consenso, ricevere - al solo costo dell'eventuale supporto utilizzato i propri dati, forniti al Titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico, qualora ciò sia tecnicamente ed economicamente possibile.

8.2 Limiti all'esercizio dei diritti

In considerazione delle modalità della videosorveglianza e dei tempi di conservazione delle registrazioni, i diritti dell'interessato incontrano le seguenti limitazioni.

- a) non è in concreto esercitabile il diritto di aggiornamento o integrazione, nonché il diritto di rettifica, di cui all'articolo 16 del GDPR, posto che le immagini sono raccolte in tempo reale e riguardano fatti obiettivi;
- b) non è esercitabile il diritto alla portabilità dei dati, di cui all'articolo 20 del GDPR, in quanto le immagini acquisite con il sistema di videosorveglianza, salvo eccezioni, non possono essere trasferite ad altri soggetti;
- c) non è esercitabile il diritto di accesso ai dati, decorsi i termini di conservazione.

8.3 Modalità di esercizio dei diritti

Per l'esercizio dei suoi diritti l'interessato può rivolgersi al Titolare, al Responsabile esterno del trattamento, ovvero al Responsabile della protezione dei dati, ai recapiti indicati ai punti 1 e 4 della presente informativa.

L'interessato potrà richiedere di visionare le immagini in cui ritiene di essere stato ripreso esibendo, o allegando alla richiesta, idonei documenti di riconoscimento. La risposta a una richiesta di accesso non potrà comprendere eventuali dati riferiti a terzi, a meno che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

Qualora intenda avvalersi di eventuali registrazioni (ad es., per la tutela di un diritto in giudizio), dovrà proporre apposita domanda scritta, corredata dalla documentazione comprovante la legittimità della richiesta (per es. estremi di denuncia-querela, estremi di un procedimento di cui è parte in causa, ordine di una Autorità).

Trovano applicazione le modalità e le procedure previste dal Disciplinare.

All'interessato è inoltre riconosciuto il diritto di presentare un reclamo al Garante per la protezione dei dati personali, ex art. 77 del GDPR, secondo le modalità previste dall'Autorità stessa (in <http://www.garanteprivacy.it>), nonché, secondo le vigenti disposizioni di legge, adire le opportune sedi giudiziarie, a norma dell'art. 79 del GDPR.

Ultima revisione: luglio 2026

**MODULO PER ACCESSO DEL TITOLARE O DI UN SUO DELEGATO
AI DATI DELLA VIDEOSORVEGLIANZA**

Al Responsabile del Servizio di Videosorveglianza
Propria sede

Il sottoscritto _____

- In qualità di Legale Rappresentante del Titolare del trattamento o suo incaricato, in base a delega scritta

Chiede di verificare le registrazioni di immagini riprese dalle ore _____ del giorno _____

alle ore _____ del giorno _____ nei seguenti luoghi di possibile ripresa:

In caso di **accertamento positivo**, chiede di procedere alle seguenti operazioni:

- ☐ conservare temporaneamente le immagini, in attesa di ulteriori disposizioni.
- ☐ realizzare copia delle registrazioni su di un supporto esterno. I supporti saranno ritirati direttamente dal sottoscritto richiedente . In caso di impedimento, saranno comunicate le generalità dell'incaricato al ritiro delle copie.
- ☐ consentire l'accesso visivo a Forze dell'Ordine, comunicando immediatamente la eventuale richiesta verbale di realizzazione e/o consegna di copie.
- ☐ consentire l'accesso visivo al Funzionario Istruttore dei procedimenti disciplinari.
- ☐ procedere alla cancellazione immediata delle immagini.

In caso di **accertamento negativo**, chiede di precisarne i motivi.

Luogo e data _____ Firma _____

(Spazio da compilare a cura del ricevente)

Luogo e data _____ **alle ore** _____ **il**
Titolare _____ **ha richiesto la ricerca di immagini eventualmente**
registrate e il compimento delle operazioni sopra indicate.

Per il ricevente *(Riportare i dati del Responsabile esterno nominato)*

_____.

Firma dell’Incaricato _____.

MODULO PER L'ACCESSO DELLE AUTORITÀ O DELLE FORZE DELL'ORDINE A DATI/IMMAGINI DELLA VIDEOSORVEGLIANZA

Al Titolare del Trattamento dei dati personali, **CCIAA di Reggio Calabria** tramite

- ☐ **Per la CCIAA di Reggio Calabria**
- ☐ **(Indicare i dati identificativi del)** Responsabile designato ex art. 28 del GDPR n. 679/2016

RICHIESTA DI ACQUISIZIONE DI IMMAGINI EVENTUALMENTE REGistrate, DA PARTE DI AUTORITÀ.

Il sottoscritto _____

In qualità di pubblico ufficiale di *(Indicare istituzione, stazione, nucleo operativo o comando di appartenenza, qualifica o grado)* _____

In riferimento alla necessità di conservare eventuali immagini registrate, per un periodo superiore 24 ore dalla loro rilevazione, nell'ambito di indagini e accertamenti da parte di Autorità e Forze dell'Ordine, ovvero di procedimenti in corso innanzi l'Autorità Giudiziaria, di sussistenza di una situazione di pericolo grave e imminente, con particolare riferimento a *(Indicare estremi del provvedimento/procedimento e dell'Autorità)*:

CHIEDE di verificare le registrazioni di immagini riprese dalle ore _____ del giorno _____
alle ore _____ del giorno _____ nei seguenti luoghi di possibile ripresa:

In caso di accertamento positivo, **CHIEDE** *(Barrare la casella di interesse)*

- ☐ di conservare temporaneamente le immagini, in attesa di ulteriori disposizioni da parte dell'Autorità.
- ☐ di acquisire copia delle registrazioni. Saranno comunicate le generalità del pubblico ufficiale incaricato al ritiro delle copie, se persona diversa dall'odierno richiedente.

Ogni comunicazione in merito alla presente domanda può essere inoltrata al sopra indicato recapito o ai seguenti contatti: telefono o fax: _____, indirizzo E-mail: _____

Data e luogo _____ Firma _____

(Spazio da compilare a cura del ricevente)

In data _____ alle ore _____ il Sig. _____

ha avanzato richiesta di accesso a immagini eventualmente registrate, in ambito di indagini e accertamenti.

Per il ricevente:

☐ per la CCIAA di Reggio Calabria

☐ (Indicare i dati identificativi del) Responsabile designato ex art. 28 del GDPR n. 679/2016

(Firma dell'Incaricato) _____.

**MODULO PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO AI DATI/IMMAGINI DELLA
VIDEOSORVEGLIANZA**

Al Titolare del Trattamento dei dati personali **CCIAA** di Reggio Calabria tramite (*Indicare a chi viene consegnato il modulo, barrando la casella di interesse*)

- ☐ **CCIAA di Reggio Calabria**
- ☐ (**Indicare i dati identificativi del**) Responsabile designato, ex art. 28 del GDPR, domiciliato c/o il Titolare.

RICHIESTA DI RICERCA DI IMMAGINI EVENTUALMENTE REGistrate, EX ART. 15 DEL GDPR

Il sottoscritto _____

Documento di identità tipo e n. _____ (*Allegare in copia al presente*)

Residente in _____

CHIEDE ai sensi dall'art. 15 del GDPR, di verificare se esistono registrazioni di immagini afferenti a se stesso e/o a suoi beni materiali, riprese dalle ore _____ del giorno _____ alle ore _____ del giorno _____ nei seguenti luoghi di possibile ripresa:

Per consentire l'eventuale reperimento delle immagini, fornisce le seguenti informazioni:

1. Attività svolta durante le riprese:

2. Altri elementi atti a facilitarne l'individuazione (*Abbigliamento, presenza di veicoli, accessori e oggetti, etc.*):

3. Presenza di altre persone nel luogo e nella fascia oraria indicati:

ALL. 6 – ESERCIZIO DEI DIRITTI DELL'INTERESSATO

In caso di **accertamento positivo** chiede (*Barrare la casella di interesse*)

- ☐ La cancellazione immediata delle immagini.
- ☐ La conservazione delle immagini per ordine di una Autorità, nell'ambito della tutela di un diritto in giudizio o di indagini da parte delle Forze dell'Ordine, accertata la sussistenza di uno stato di pericolo concreto ed imminente. A tal fine, indica gli estremi dell'Autorità e del relativo atto, che legittima la conservazione delle immagini e la successiva acquisizione di eventuali copie:

- ☐ La conservazione delle immagini per le esigenze della difesa in giudizio in un procedimento penale, ai sensi dell'art. 391 quater del cod. proc. pen. A tal fine, allega la richiesta dell'avvocato difensore dell'interessato:

Inoltre, chiede che ogni comunicazione in merito alla presente domanda sia indirizzata al sopra indicato indirizzo o ai seguenti contatti:

Telefono o fax: _____

Indirizzo E-mail/PEC: _____

Il sottoscritto dichiara di aver ricevuto, in copia cartacea in allegato al presente modulo, **adeguata informativa ex art. 13 del GDPR**. In proposito, **dichiara di aver compreso che:**

- ✓ *Il periodo massimo di conservazione delle immagini è di 24 ore dalla loro rilevazione. Decorso questo termine, in assenza di un atto che ne legittimi la ulteriore conservazione, si procederà a cancellarle, a norma di legge.*
- ✓ *Le copie delle eventuali registrazioni saranno consegnate soltanto alle Forze dell'Ordine, previa richiesta formale di acquisizione da parte dell'Autorità (salvo espresso ordine di consegna all'interessato).*
- ✓ *La videosorveglianza è una misura funzionale a tutelare i beni aziendali e a rilevare eventuali situazioni di pericolo, complementare e non sostitutiva rispetto all'attività della Magistratura o delle Forze dell'Ordine. Pertanto, non comporta alcun obbligo né aspettativa di tutela di beni estranei al patrimonio del Titolare.*

Data e luogo _____ Firma _____

(*Spazio da compilare a cura del ricevente*)

Luogo e data _____ **alle ore** _____ **il Sig.** _____
ha avanzato richiesta di accesso alle immagini eventualmente

ALL. 6 – ESERCIZIO DEI DIRITTI DELL'INTERESSATO

registrate. Il Titolare risponderà nei termini di legge. I dati forniti con il presente modulo saranno trattati per le sole finalità di agevolare l'esercizio dei diritti di cui all'art. 15 del GDPR.

Per il ricevente:

☐ URP– Reception CCIAA di Reggio Calabria

☐ (Indicare i dati identificativi del) Responsabile designato ex art. 28 del GDPR

(Firma dell'Incaricato) _____.

VERBALE DI CONSEGNA COPIA DI IMMAGINI REGISTRATE

A seguito di richiesta / autorizzazione, da parte del Titolare del trattamento, **CCIAA di Reggio Calabria**, prot. _____ del _____ (*Allegare in copia al presente verbale*)

Io sottoscritto _____, in qualità di persona autorizzata dal Titolare:

(*Cognome e Nome*) _____,

documento di identità n. _____ (*Allegare in copia al presente verbale*),

in qualità di _____ (*Ruolo o mansioni*)

AUTORIZZATO per lo specifico ambito di trattamento dei dati.

(*Oppure, se Pubblico Ufficiale autorizzato all'acquisizione delle copie*):

☐ (*Cognome e Nome*) _____,

in qualità di _____ (*Ruolo o grado*)

Stazione/ Comando / Unità operativa

(*Oppure, se Avvocato autorizzato all'acquisizione delle copie*):

☐ (*Cognome e Nome*) _____,

in qualità di _____,

ai sensi del _____, ovvero sulla base del provvedimento dell'Autorità _____
del _____,

ricevo da (*Indicare i dati identificativi del*), Responsabile esterno designato, ex art. 28 del GDPR, tramite soggetto

autorizzato appartenente alla sua organizzazione, Sig.

copia della registrazione, effettuata ed estrapolata a norma di legge, delle immagini riprese:

✓ dalle ore _____ del giorno _____

✓ alle ore _____ del giorno _____

e pertanto riversate in supporto asportabile del tipo _____ (*Indicare se CD, chiavetta
USB, hard disk esterno o altro*).

Luogo e data _____

(Firma di chi ritira le copie)

(Firma di chi consegna le copie)

CLASSIFICAZIONE DEI SOGGETTI AUTORIZZATI E MODELLO DI REGISTRO DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO PER LA VIDEOSORVEGLIANZA

1. Classificazione dei soggetti autorizzati

I soggetti autorizzati al trattamento dei dati personali relativi alla videosorveglianza, sono classificati in base ai seguenti profili di autorizzazione:

Profilo di autorizzazione corrispondente all'ambito di trattamento		Sono incaricati a questo specifico ambito di trattamento:
(A)	Visione in tempo reale delle immagini sui monitor, senza accesso alle registrazioni	Il personale al quale, in ragione delle mansioni affidate, compete esclusivamente il monitoraggio delle immagini riprese in tempo reale. Questo gruppo di Incaricati non può e non deve accedere alle registrazioni, estrarne copia o cancellarle, amministrare, configurare o gestire il sistema.
(B)	Accesso visivo alle registrazioni	Il personale deputato alle operazioni di ricerca e visione, delle immagini registrate. Per ragioni operative, questo gruppo di Incaricati può anche visionare le immagini in tempo reale (il profilo B assorbe il profilo A). Non può e non deve realizzare copie di sicurezza, né amministrare, configurare o gestire il sistema.
(C)	Ricerca e visione e delle immagini registrate, realizzazione delle copie di sicurezza	Il personale deputato alle operazioni di ricerca, visione, estrazione e riproduzione (anche tramite la realizzazione di copie su CD o DVD, o altro supporto, da mettere a disposizione delle Forze dell'Ordine o dell'Autorità Giudiziaria) delle immagini registrate. Per ragioni operative, questo gruppo di Incaricati può anche visionare le immagini in tempo reale (il profilo C assorbe i profili A, B e C). Non può e non deve amministrare né configurare il sistema.
(D)	Amministrazione del sistema digitale di videosorveglianza con registrazione	Il personale tecnico (interno o dipendente della ditta installatrice), per le operazioni di gestione ed amministrazione del sistema, compresa la configurazione delle videocamere e del registratore digitale. Possono visionare le immagini (live o registrate) solo se necessario, ai fini e nei limiti dell'intervento che devono compiere.

(E)	Manutenzione preventiva e correttiva del sistema	Il personale tecnico (interno o dipendente della ditta installatrice), per le operazioni di manutenzione del software e dell'hardware. Possono visionare le immagini (live o registrate) solo se necessario, ai fini e nei limiti dell'intervento che devono compiere.
-----	--	--

L'atto di individuazione dei soggetti autorizzati dovrà contenere il riferimento al profilo di trattamento attivato.

Gli addetti possono essere identificati direttamente dal Titolare ovvero dal Responsabile esterno designato.

In alternativa, il fornitore può inviare una lista nominativa dei propri incaricati, con riferimento ai profili di accesso e autorizzazione precedentemente definiti, con attestazione della loro avvenuta formazione in argomento.

Al manutentore / installatore può essere richiesto di sottoscrivere un apposito impegno di riservatezza, in aggiunta a quanto già espresso per vincolo contrattuale e dovere professionale ex lege.

2. Modello di Registro dei soggetti autorizzati

Di seguito si propone un modello di Registro dei soggetti autorizzati ai trattamenti per la videosorveglianza.

