

LOGO COMUNE

Comune di ...



Arma dei Carabinieri

**PROTOCOLLO OPERATIVO PER LA DISCIPLINA DEL TRATTAMENTO
DEI DATI PERSONALI NELL'AMBITO DEL SISTEMA DI
VIDEOSORVEGLIANZA URBANA [EVENTUALE: E LETTURA TARGHE]**

TRA

COMUNE di ...

E

COMANDO PROVINCIALE CARABINIERI DI ...

[EVENTUALE – in caso di adesione delle altre Forze di polizia*]

LA QUESTURA DI ...

IL COMANDO PROVINCIALE DELLA GUARDIA DI FINANZA DI ...

* *N.B. > L'adesione della Polizia di Stato (tramite la Questura competente) e del Corpo della Guardia di Finanza al presente protocollo operativo può trovare applicazione nei centri urbani caratterizzati da compresenza istituzionale dei rispettivi presidi territoriali, circostanza che ricorre tipicamente nei Comuni capoluogo di provincia o in quelli sede di Commissariato di P.S. e di articolazioni della GDF (Gruppo o Compagnia). Negli altri contesti comunali, il protocollo si perfeziona in via bilaterale tra il Comune e l'Arma dei Carabinieri, formalmente siglato dal Comandante Provinciale, d'intesa con la Prefettura-UTG. Sotto il profilo tecnico-operativo, l'interconnessione e l'accesso ai flussi video sono strutturati per confluire direttamente presso la Centrale Operativa del Comando Provinciale ovvero presso la Centrale Operativa della Compagnia Carabinieri territorialmente competente sul Comune interessato.*

Il Sindaco *pro tempore* del Comune di [Nome Comune] e il Comandante Provinciale dell'Arma dei Carabinieri di [Nome Provincia], [EVENTUALE] (*il Questore di [Nome Provincia] e il Comandante Provinciale della Guardia di Finanza di [Nome Provincia]*):

CONSIDERATO

- che, per garantire adeguati livelli di sicurezza urbana, i soggetti istituzionali, a diverso titolo competenti, sono chiamati, nel rispetto di specifiche attribuzioni, a sviluppare in forma coordinata interventi volti alla prevenzione della criminalità, in particolare di quella predatoria;
- che la Corte Costituzionale, nella sentenza 12 novembre 2020, n. 236, ha ribadito che la prevenzione dei reati e il controllo del territorio costituiscono il nucleo Centrale della funzione di pubblica sicurezza, di competenza esclusivamente statale, a mente dell'articolo 117, secondo comma, lettera h), della Costituzione e demandata dalla legge 1° aprile 1981, n. 121 alle Autorità di pubblica sicurezza ed alle Forze di polizia;
- che il Comune di [Nome Comune] ha progettato e realizzato un sistema di videosorveglianza urbana [EVENTUALE] (*e un sistema di lettura targhe per il rilevamento anche automatizzato delle violazioni in materia di circolazione stradale*) che intende impiegare al fine di contribuire ad innalzare il livello della sicurezza urbana;
- che il trattamento dei dati personali effettuato dal Comune mediante il predetto sistema di videosorveglianza [EVENTUALE] (*e il sistema di lettura targhe*), essendo finalizzato alla tutela della sicurezza urbana, è disciplinato dal Regolamento (UE) 2016/679 (GDPR), ed è altresì accessibile alla Polizia Municipale per l'assolvimento delle funzioni di polizia giudiziaria ai sensi del decreto legislativo 18 maggio 2018, n. 51;
- che è intendimento del Comune attivare un collegamento con le Sale o Centrali operative delle Forze di polizia per consentire la visione delle immagini in tempo reale (live) e in differita, [EVENTUALE] (*nonché un collegamento con la Questura per consentire la comunicazione dei dati raccolti dal proprio sistema di lettura targhe al Centro Elettronico Nazionale della Polizia di Stato - CEN, ai fini dell'elaborazione informatica da parte del "Sistema di controllo nazionale targhe e transiti" - SCNTT*);
- che il Comune di [Nome Comune] e la Prefettura-UTG di [Nome Provincia], in data ... hanno sottoscritto il "Patto per l'attuazione della sicurezza urbana", con cui è stata condivisa la cornice strategica per l'implementazione e l'interconnessione dell'impianto di videosorveglianza;
- che l'art. 2 del menzionato Patto individua quale prioritario obiettivo l'installazione e il potenziamento dei sistemi di videosorveglianza comunali [EVENTUALE] (*e lettura targhe*) nelle aree maggiormente interessate da fenomeni di illegalità, specificamente finalizzati alle azioni di prevenzione e di contrasto della criminalità diffusa e predatoria;
- che, in aderenza a quanto previsto dallo stesso Patto e in conformità ai criteri di indirizzo fissati dalle disposizioni ministeriali, il progetto tecnico del sistema di videosorveglianza [EVENTUALE] (*e lettura targhe*) del Comune di [Nome

Comune] è stato oggetto di preventiva e favorevole valutazione da parte del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica (CPOSP), in relazione alle modalità di impiego, all'efficacia del contesto urbano ed a ogni aspetto tecnico-operativo;

- che l'articolo 3 del Patto istituisce presso la Prefettura-Ufficio Territoriale del Governo una Cabina di regia, composta dai rappresentanti delle Forze di polizia e della Polizia locale, con il compito di monitorare lo stato di attuazione del sistema e l'efficacia delle strategie congiunte adottate;
- che le vigenti norme in materia impongono di prevedere la titolarità disgiunta dei trattamenti dei dati personali acquisiti attraverso il sistema di videosorveglianza, in ragione delle differenti finalità per le quali i medesimi trattamenti sono effettuati;

VISTI

- il Regolamento (UE) 2016/679 (GDPR);
- il decreto legislativo 18 maggio 2018, n. 51;
- il D.P.R. 15 gennaio 2018, n. 15;
- il Codice in materia di protezione dei dati personali (D.Lgs. 196/2003);
- la legge 1° aprile 1981, n. 121 e l'articolo 159 del D.Lgs. 15 marzo 2010, n. 66 concernente i compiti di istituto dell'Arma dei Carabinieri;
- il decreto-legge 20 febbraio 2017, n. 14, convertito dalla legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città";
- la circolare del Ministero dell'Interno - Ufficio Coordinamento e Pianificazione delle Forze di Polizia n. 558/SICPART/421.2/70/224632 del 2 marzo 2012, recante "Sistemi di videosorveglianza in ambito comunale - Direttiva" e l'annessa "Piattaforma della videosorveglianza integrata";
- [EVENTUALE] *(la circolare del Dipartimento della Pubblica Sicurezza n. 0001065 del 12 gennaio 2018 relativa alla realizzazione dei sistemi di lettura targhe ed integrazione allo SCNTT)*;

CONVENGONO QUANTO SEGUE

Capo I

Disposizioni generali

Art. 1

Ambito di applicazione

1. Con il presente protocollo operativo, il Comune di [Nome Comune] e il Comando Provinciale dei Carabinieri di [Nome Provincia] [EVENTUALE] *(e le altre Forze di polizia aderenti)* definiscono le modalità di utilizzazione del sistema di videosorveglianza [EVENTUALE] *(e del sistema di lettura targhe)*.
2. Il presente protocollo definisce i termini secondo i quali i dati della videosorveglianza sono resi disponibili alla Centrale operativa dell'Arma dei Carabinieri [EVENTUALE] *(e delle altre Forze di Polizia)* per l'espletamento dei compiti di prevenzione e repressione dei reati e tutela dell'ordine pubblico.

[EVENTUALE] *(Definisce ancora i termini secondo i quali i dati raccolti dal sistema di lettura targhe sono comunicati al CEN della Polizia di Stato per l'elaborazione informatica da parte dello SCNTT).*

3. Le premesse fanno parte integrante del presente atto.

Art. 2

Definizioni

Ai fini del presente protocollo, si intende per:

- “Codice della strada”: il nuovo Codice della strada di cui al decreto legislativo 30 aprile 1992, n. 285;
- “Comune”: il Comune di [Nome Comune];
- “D.Lgs. 51/2018”: il decreto legislativo 18 maggio 2018, n. 51;
- “Parti”: il Comune di [Nome Comune] e le Forze di polizia collegate al sistema di videosorveglianza;
- “Comando Provinciale”: il Comando Provinciale dell’Arma dei Carabinieri di [Nome Provincia] e [EVENTUALE] *(il Comando Provinciale della Guardia di Finanza di [Nome Provincia] o altra articolazione territoriale competente);*
- “Questura”: la Questura di [Nome Provincia];
- “Regolamento UE n. 679 del 2016 (GDPR)”: il Regolamento generale sulla protezione dei dati (GDPR);
- “Sicurezza urbana”: il bene pubblico che afferisce alla vivibilità e al decoro delle città, cui concorrono lo Stato e gli enti locali nel rispetto delle rispettive competenze;
- “Sistema di videosorveglianza”: l’infrastruttura di ripresa installata dal Comune per finalità di sicurezza urbana;
- [EVENTUALE] *(“Sistema di lettura targhe”: il sistema per il riconoscimento automatizzato delle targhe per il rilevamento delle violazioni in materia di circolazione stradale;)*
- “Accesso”: l’operazione elettronica che consente di prendere visione e di estrarre copia dei dati raccolti;
- [EVENTUALE] *(“CEN”: il Centro Elettronico Nazionale della Polizia di Stato; “SCNTT”: il Sistema di controllo nazionale targhe e transiti, gestito dal CEN;)*
- “Dati resi disponibili”: i dati raccolti dal Comune e resi accessibili per via telematica alle Centrali/Sale operative dei Titolari autonomi.

Art. 3

Finalità dei trattamenti

1. I dati personali raccolti dal sistema di videosorveglianza sono trattati dal Comune per il tramite del dipendente Corpo (o Servizio) di Polizia Municipale, per le finalità connesse alle funzioni ed ai compiti di sicurezza urbana attribuiti dalla legge ai Comuni.
2. [EVENTUALE] *(I dati personali raccolti dal sistema di lettura targhe sono trattati dal Comune per il tramite della dipendente Polizia Municipale, per le finalità amministrative di rilevamento delle violazioni in materia di circolazione stradale, in relazione alla competenza ad espletare i servizi di polizia stradale,*

attribuita dall'articolo 12 del Codice della strada ai Corpi e ai servizi di polizia Municipale, nell'ambito del territorio di competenza.)

3. I dati personali raccolti con i sistemi di cui al comma 1 [EVENTUALE] *(e al comma 2)* sono resi disponibili alla Polizia Municipale, che può ulteriormente utilizzarli per l'assolvimento, nell'ambito territoriale di competenza, delle funzioni di polizia giudiziaria attribuite dall'articolo 5, comma 1, lettera a) della legge 7 marzo 1986, n. 65.
4. Il Comando Provinciale dell'Arma dei Carabinieri *(o altra articolazione territoriale dipendente)* [EVENTUALE] *(la Questura o altro ufficio periferico della Polizia di Stato e il Comando Provinciale della Guardia di Finanza o altro Reparto territoriale dipendente)* può [EVENTUALE] *(possono)* trattare i dati personali, resi disponibili per le finalità di cui al comma 1, per finalità 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, di cui all'articolo 1, comma 2, del decreto legislativo n. 51 del 2018.
5. [EVENTUALE] *(Il CEN può trattare i dati personali di cui al comma 2, comunicati dal Comune, per finalità 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, di cui all'articolo 1, comma 2, del decreto legislativo n. 51 del 2018.)*

Art. 4

Principi generali e regole di trattamento dei dati personali

1. Le Parti concordano sulla necessità che i trattamenti per finalità amministrative effettuati dal Comune siano compiuti nel rispetto del GDPR e del Codice in materia di protezione dei dati personali, e che gli ulteriori trattamenti effettuati dall'Arma dei Carabinieri [EVENTUALE] *(e dalle altre Forze di polizia aderenti)* siano compiuti nel rispetto delle regole e dei principi di cui al D.Lgs. 51/2018 e al D.P.R. 15 gennaio 2018, n. 15.
2. Il Comune dà atto di aver effettuato la necessaria valutazione d'impatto (DPIA) di cui all'articolo 35 del GDPR, prima di procedere al trattamento dei dati raccolti in modo sistematico nelle zone accessibili al pubblico mediante il sistema di videosorveglianza [EVENTUALE] *(e il sistema di lettura targhe)*.
3. Il Comune dà altresì atto di aver adottato diversificati livelli di visibilità e di trattamento delle immagini da parte del personale abilitato attraverso credenziali di autenticazione individuale, al fine di verificare costantemente l'attività espletata.
4. Le Parti danno atto che l'Arma dei Carabinieri [EVENTUALE] *(e le altre Forze di polizia aderenti)*, in conformità alle politiche interne sulla protezione dei dati, adotta [EVENTUALE] *(adottano)* la necessaria valutazione d'impatto prevista dall'articolo 23 del D.Lgs. 51/2018. In ragione della sostanziale omogeneità e similarità delle modalità operative, l'Arma dei Carabinieri si avvale [EVENTUALE] *(e ciascuna Forza di polizia si avvale per quanto di propria competenza)* della facoltà di effettuare un'unica e distinta valutazione d'impatto a

livello nazionale, valida per la totalità dei sistemi di videosorveglianza urbana capillarmente interconnessi sul territorio.

5. Ciascun titolare del trattamento, nell'ambito dei trattamenti di rispettiva pertinenza, assicurerà in via diretta l'esercizio dei diritti degli interessati.

Art. 5

Titolari dei trattamenti

1. Il Comune è il titolare del trattamento dei dati personali effettuato mediante il sistema di videosorveglianza per le finalità di sicurezza urbana di cui all'articolo 3, comma 1. [EVENTUALE] *(È altresì titolare del trattamento effettuato mediante il sistema di lettura targhe per le finalità di cui all'articolo 3, comma 2).*
2. Il Comune è anche titolare dell'ulteriore trattamento dei dati resi disponibili al dipendente Corpo (o servizio) di Polizia Municipale per l'assolvimento degli obblighi di polizia giudiziaria ex art. 5, comma 1, lett. a) della legge 65/1986.
3. L'Arma dei Carabinieri [EVENTUALE] *(e il Ministero dell'Interno - Dipartimento della pubblica sicurezza e al Corpo della Guardia di Finanza) è [EVENTUALE] (sono) autonomo titolare [EVENTUALE] (autonomi titolari) dei trattamenti dei dati personali raccolti dal sistema di videosorveglianza effettuati dalle rispettive articolazioni territoriali per le finalità di polizia di cui all'articolo 3, comma 4.*
4. [EVENTUALE] *(Il Ministero dell'Interno - Dipartimento della pubblica sicurezza è autonomo titolare del trattamento dei dati personali raccolti dal sistema di lettura targhe e comunicati dal Comune, effettuato dal CEN mediante l'SCNTT, per le finalità di cui all'articolo 3, comma 5.)*
5. I Titolari adottano, in conformità a quanto previsto dall'**Allegato A**, misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio di violazioni di sicurezza che comportino, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali comunque trattati.
6. Fermi restando gli obblighi di notifica all'Autorità Garante per la protezione dei dati personali, al verificarsi di una violazione di sicurezza (data breach), il titolare che la rileva ne dà immediata comunicazione agli altri titolari al fine di adottare le necessarie misure di contenimento.

Art. 6

Autorizzati ai trattamenti

1. Le persone che agiscono sotto l'autorità diretta dei titolari del trattamento non possono avere accesso ai dati personali se non sono state previamente autorizzate e istruite in tal senso. L'autorizzazione è documentata per iscritto e descrive nel dettaglio l'ambito di trattamento consentito, definendo diversi livelli di visibilità e trattamento dei dati in funzione dei compiti attribuiti ai singoli operatori.
2. L'autorizzazione al trattamento di cui al comma 1 è adottata:
 - per il Comune, nell'ambito del personale del Corpo (o Servizio) di Polizia Municipale, dal Comandante (o Responsabile);

- per l'Arma dei Carabinieri, dal Comandante Provinciale o, su sua delega, dal Comandante del Reparto Operativo, ovvero dal Comandante del reparto territoriale da cui dipende la Centrale Operativa, nell'ambito del personale dipendente;
- [EVENTUALE] (*per il Ministero dell'Interno - Dipartimento della pubblica sicurezza, dal Questore o dal Dirigente di altro ufficio periferico della Polizia di Stato o, su sua delega, nell'ambito del personale della Polizia di Stato dipendente;*)
- [EVENTUALE] (*per la Guardia di Finanza, dal Comandante Provinciale o, su sua delega, dal Comandante del Reparto territoriale dipendente.*)

Capo II

Caratteristiche generali del sistema di videosorveglianza [EVENTUALE] (e del sistema di lettura targhe)

Art. 7

Caratteristiche tecniche del sistema di videosorveglianza

1. Le caratteristiche tecniche del sistema di videosorveglianza [EVENTUALE] (*e del sistema di lettura targhe*) sono definite dal documento in **Allegato B** al presente protocollo operativo¹, di cui è parte integrante, ove deve essere indicata anche l'ubicazione delle telecamere. Le Parti danno atto che le informazioni relative all'ubicazione delle telecamere potranno essere fornite attraverso modalità di georeferenziazione su cartografia digitale, integrate nel sistema.
2. Le Parti danno atto che il sistema di videosorveglianza è configurato in modo da consentire alla Centrale operativa del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*e alle Sale o Centrali operative della Questura o altro ufficio periferico della Polizia di Stato e del Comando Provinciale del Corpo della Guardia di Finanza o altra articolazione territoriale dipendente*) di accedere in tempo reale (live) al predetto sistema e alle immagini da esso riprese secondo le modalità selettive individuate dall'articolo 9, commi 2 e 3.
3. Le Parti danno inoltre atto che gli accessi e le operazioni sul server ove sono conservate le registrazioni del sistema di videosorveglianza, effettuati dal personale autorizzato dal Comune con le modalità di cui all'articolo 6, comma 2, sono registrati in appositi file di log, non modificabili, conservati dal Comune per tre anni e con un minimo di 12 mesi dall'accesso e dall'operazione, resi accessibili per la verifica della liceità del trattamento, del controllo interno e nell'ambito del procedimento penale.

Art. 8

Informativa concernente il sistema di videosorveglianza

1. Il Comune assicura che l'informativa agli interessati che stanno per accedere in una zona videosorvegliata [EVENTUALE] (*o nel raggio d'azione del lettore targhe*) è fornita, ai sensi dell'articolo 13 del Regolamento (UE) n. 679/2016,

¹ I contenuti dell'Allegato B devono essere determinati a seconda delle soluzioni tecniche implementate dal Comune.

attraverso la collocazione di cartelli di avvertimento conformi al modello semplificato di informativa “minima” definita dal Garante per la protezione dei dati personali (primo livello). Tale informativa “minima” rimanda all’informativa completa e dettagliata di cui al menzionato articolo 13 (secondo livello), messa a conoscenza degli interessati mediante pubblicazione sul sito web istituzionale del Comune [EVENTUALE] (*accessibile anche con QR-code inserito nel cartello di avvertimento*).

2. L’attivazione del collegamento con la Centrale operativa dell’Arma dei Carabinieri [EVENTUALE] (*e con le Centrali/Sale operative della Polizia di Stato e del Corpo della Guardia di Finanza*) è resa nota agli interessati mediante l’informativa (di primo e secondo livello) di cui al comma 1.

Art. 9

Collegamento del sistema alla Centrale operativa dell’Arma dei Carabinieri [EVENTUALE] (e alle Sale o Centrali operative della Questura e del Corpo della Guardia di Finanza)

1. Le Parti danno atto del fatto che il collegamento del sistema di videosorveglianza alle soluzioni tecnologiche adottate dalla Centrale operativa del Comando Provinciale dell’Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*e dalle Sale o Centrali operative della Questura o altro ufficio periferico della Polizia di Stato e del Comando Provinciale del Corpo della Guardia di Finanza o altra articolazione territoriale dipendente*), avviene per mezzo di una rete telematica dedicata.
2. Il collegamento consente al personale della Centrale operativa del Comando Provinciale dell’Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*e della Sala/Centrale operativa della Questura o altro ufficio periferico della Polizia di Stato*), per le finalità di cui all’art. 3, comma 4, del presente protocollo operativo, di accedere alle telecamere e visionare le immagini in tempo reale (live), in presenza degli eventi o delle situazioni indicate nell’Allegato C, accluso al presente testo.
3. [EVENTUALE] (*Il collegamento consente al personale autorizzato delle Sale o Centrali operative del Comando Provinciale del Corpo della Guardia di Finanza o altra articolazione territoriale dipendente di accedere, per le finalità di cui all’art.3, comma 4, del presente protocollo, limitatamente alle attribuzioni del medesimo Corpo, di accedere alle telecamere e visionare le immagini in tempo reale live, in presenza degli eventi o delle situazioni indicate nell’Allegato D, accluso al presente testo.*).
4. Il collegamento consente al personale autorizzato della Centrale operativa di cui al comma 1, nonché ad altro personale appositamente individuato dipendente dal Comando Provinciale dell’Arma dei Carabinieri [EVENTUALE] (*ovvero dalla Questura o dal Corpo della Guardia di Finanza*), di accedere alle immagini in differita ed estrarne copia, con connessione da remoto al server ove sono conservate le registrazioni raccolte dal sistema di videosorveglianza comunale. L’estrazione di copia delle immagini è oggetto di apposita registrazione, anche attraverso la redazione di sommari verbali delle operazioni compiute.

5. Le Parti danno inoltre atto che il Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*la Questura o altro ufficio periferico della Polizia di Stato e il Comando Provinciale del Corpo della Guardia di Finanza o altro Reparto territoriale dipendente*) adotta [EVENTUALE] (*adottano*) diversificati livelli di visibilità e di trattamento delle immagini da parte del personale autorizzato di cui all'articolo 6, il quale è abilitato, attraverso il rilascio di credenziali di autenticazione individuale, a compiere le sole operazioni correlate ai compiti assegnati. Le credenziali per accedere al server sono rilasciate in forma anonima dal Comune e consegnate al referente di ciascuna Forza di polizia per la successiva assegnazione nominativa, di cui dovrà essere tenuta apposita registrazione.
6. Le operazioni di visione ed estrazione delle immagini di cui ai commi 2, 3 e 4 e le esigenze che le hanno rese necessarie sono annotate, anche in modalità automatizzata, nel registro della Centrale operativa e delle altre unità operative interessate.
7. Le Parti danno altresì atto che gli accessi e le operazioni effettuate dal personale del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*e della Questura o altro ufficio periferico della Polizia di Stato e del Comando Provinciale del Corpo della Guardia di Finanza o altro Reparto territoriale dipendente*) sul server comunale sono registrati in appositi file di log, non modificabili, conservati dal Comune per [da concordare, preferibilmente 3 anni] dall'accesso e dall'operazione, resi accessibili ai predetti Uffici e Comandi per la verifica della liceità del trattamento, del controllo interno e nell'ambito del procedimento penale.

Art. 10

Personale addetto alla gestione e manutenzione del sistema di videosorveglianza

1. Le Parti danno atto che la gestione, la manutenzione e l'aggiornamento del sistema di videosorveglianza [EVENTUALE] (*e del sistema di lettura targhe*) sono garantite dal Comune, quale proprietario del sistema, attraverso personale tecnico appositamente incaricato, al quale non è consentito accedere alle risorse informative e alle immagini memorizzate nel sistema, salvo comprovate e documentate esigenze tecniche. In tal caso le operazioni avverranno alla presenza e sotto il controllo del personale del Comune.
2. Al termine di ciascun intervento di manutenzione, il responsabile dell'operazione rilascia al Comune una dichiarazione scritta relativa all'attività svolta.
3. [EVENTUALE] (*Le Parti danno atto che, con riferimento alla comunicazione del Comune dei dati raccolti dal sistema di lettura targhe, gli interventi che rendano necessario l'accesso fisico o logico al server collettore ubicato in Questura o in altro ufficio periferico della Polizia di Stato siano previamente concordati ed eseguiti alla presenza dell'amministratore di sistema o altro tecnico della Questura. In tali casi il personale tecnico incaricato rilascia attestazione scritta delle operazioni eseguite*).
4. [EVENTUALE] (*Le Parti danno atto che il Comune assicurerà l'adeguamento del sistema di lettura targhe alle prescrizioni tecniche impartite dal Dipartimento*

della pubblica sicurezza, per garantire il collegamento telematico in caso di interventi di aggiornamento tecnologico riguardanti l'SCNTT).

Capo III

Trattamento dei dati personali per finalità di sicurezza urbana

Art. 11

Ubicazione del server

1. Le Parti danno atto che il server presso il quale sono memorizzati i dati personali raccolti dal sistema di videosorveglianza per finalità di sicurezza urbana, resi disponibili al Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*alla Questura o altro ufficio periferico della Polizia di Stato e al Comando Provinciale della Guardia di Finanza o altro Reparto territoriale dipendente*), è ubicato presso [le sedi individuate dal Comune].

Art. 12

[EVENTUALE - Rilevazione delle targhe dei veicoli e modalità di comunicazione al SCNTT]

1. (*Le Parti convengono che il sistema di lettura targhe comunale può essere interconnesso allo SCNTT attraverso un collegamento telematico dedicato con un server collettore installato presso la Questura (o altro ufficio periferico della Polizia di Stato) con le modalità tecniche di interfacciamento definite nell'Allegato E al presente protocollo operativo, di cui è parte integrante*)².

Art. 13

Termine di conservazione dei dati

1. La conservazione dei dati, delle informazioni e delle immagini raccolti attraverso il sistema di videosorveglianza è limitata, ai sensi dell'articolo 6, comma 8, del decreto legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione, quali quelle connesse allo svolgimento di eventuali attività di indagine delegate o coordinate dall'Autorità Giudiziaria. Decorso i termini predetti, le immagini sono cancellate automaticamente.

Capo IV

Disposizioni finali

Art. 14

Cabina di regia e monitoraggio

² Nel caso di interfacciamento tra il sistema SCNTT ed il server collettore (LPR) ubicato presso la Questura o altro ufficio territoriale della Polizia di Stato, le specifiche tecniche sono contenute nel Documento di Specifiche di Interfaccia già allegato alla Circolare del 12 gennaio 2018 richiamata in premessa.

1. Il monitoraggio sull'attuazione, sull'efficacia operativa e sulle future implementazioni tecnologiche del presente protocollo è devoluto alla Cabina di regia già istituita presso la Prefettura - U.T.G., fatta salva l'obbligatoria e preventiva valutazione del Comando Generale dell'Arma dei Carabinieri [EVENTUALE] (*e dei rispettivi Organi Centrali delle altre Forze di polizia*) circa l'eventuale impiego di sistemi di Intelligenza Artificiale per finalità di polizia, nei limiti previsti dal decreto ministeriale di cui all'art. 24, comma 2, lett. h), della legge n. 132/2025.
2. La citata Cabina di regia esamina lo stato dei collegamenti con cadenza semestrale, anche al fine di consentire al Prefetto la predisposizione della relazione informativa periodica da trasmettere al Dipartimento della Pubblica Sicurezza.
3. Per assicurare la continuità operativa ed efficientare la gestione tecnica del sistema, le Parti concordano di prevedere e aggiornare costantemente una *mailing list* dedicata alle comunicazioni urgenti tra i referenti tecnici dei Titolari autonomi (es. segnalazione di guasti agli apparati, blocchi temporanei di telecamere per indagini o disservizi legati ad aggiornamenti programmati del software).

Art. 15

Clausole di salvaguardia e pubblicazione

1. Dal presente Protocollo non derivano nuovi e maggiori oneri per l'Erario. Ha una durata di anni ... dalla sottoscrizione ed è tacitamente rinnovato.
2. A cura delle Parti firmatarie, copia del presente protocollo operativo, debitamente sottoscritta con firma digitale, viene formalmente trasmessa alla Prefettura - UTG di ... ai fini della formale notificazione dell'accordo, per l'aggiornamento della mappatura provinciale dei flussi video e per consentire le attività di verifica devolute alla Cabina di regia prefettizia di cui all'articolo 14.
3. Le controversie interpretative o esecutive sono deferite in via esclusiva al Foro territoriale di ...
4. Il presente atto è soggetto agli obblighi di pubblicazione nella sezione "Amministrazione Trasparente" del sito web istituzionale del Comune ai sensi dell'articolo 23, comma 1, lettera d), del decreto legislativo 14 marzo 2013, n. 33.

PER IL COMUNE DI ..., il Sindaco,

PER L'ARMA DEI CARABINIERI, Il Comandante Provinciale di ... ,

[EVENTUALE]

PER LA POLIZIA DI STATO, Il Questore di ... ,

PER LA GUARDIA DI FINANZA, il Il Comandante Provinciale di ... ,

**DISCIPLINARE TECNICO DELLE MISURE DI SICUREZZA
TECNICHE E ORGANIZZATIVE**

(ai sensi dell'art. 5, comma 5, del presente protocollo)

Sezione I – Misure di sicurezza e adempimenti a cura del Comune*

(quale Titolare autonomo della raccolta originaria e proprietario esclusivo degli asset hardware, software e di rete)

NOTA DI COORDINAMENTO TECNICO > L'elenco delle misure tecniche e organizzative descritte nella presente Sezione costituisce un indirizzo di massima e non ha carattere assolutamente tassativo. Tali indicazioni possono essere liberamente adattate, integrate o modificate dall'Amministrazione comunale a seconda delle soluzioni hardware, software e architetture concretamente implementate nello specifico sistema di videosorveglianza urbana (VDS) locale.

L'unico vincolo tassativo per l'Ente locale e per i suoi manutentori esterni è che le soluzioni applicate sul territorio garantiscano comunque contromisure robuste, capaci di assicurare un livello di sicurezza e protezione dei dati equivalente o superiore agli standard di riferimento.

A titolo di mero orientamento sulle best practices di settore per l'Ente e per le ditte affidatarie, si richiama l'opportunità di fare riferimento ai parametri prestazionali e strutturali minimi definiti nel "Documento Tecnico" annesso alla circolare del Ministero dell'Interno n. 558/SICPART/421.2/70/224632 del 2 marzo 2012, citata nelle premesse del presente protocollo (con particolare riguardo ai requisiti minimi per telecamere di contesto/osservazione, architetture di rete, videosever e sistemi di registrazione).

Il Comune, in relazione alle tecnologie da esso impiegate per il trattamento dei dati personali raccolti dal sistema di videosorveglianza [EVENTUALE] (e dal sistema di lettura targhe), previa valutazione dei rischi, adotta le misure volte a:

- 1) proteggere fisicamente i dati adottando idonee misure per il controllo degli accessi (es. serrature di sicurezza, badge elettronico, sistemi di riconoscimento biometrico, ecc.) e per assicurare l'affidabilità dell'infrastruttura (es. sistemi UPS, impianti antintrusione, antincendio, antiallagamento, etc.);
- 2) proteggere i flussi di comunicazione del sistema di videosorveglianza [EVENTUALE] (e di lettura targhe) attraverso la presenza di firewall perimetrali, anche con funzioni di antimalware, antivirus, antispam, al fine di evitare possibili accessi non autorizzati;
- 3) negare alle persone non autorizzate l'accesso ai dispositivi utilizzati per il trattamento dei dati;
- 4) impedire che i supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate;
- 5) impedire che i dati raccolti dal sistema di videosorveglianza [EVENTUALE] (e dal sistema di lettura targhe), siano trattati senza autorizzazione e che sia presa visione senza autorizzazione dei dati personali conservati, o che gli stessi siano modificati o cancellati o trasmessi senza autorizzazione;
- 6) garantire, in conformità a quanto stabilito dall'Articolo 9, comma 5 del presente protocollo operativo [EVENTUALE] (e dalle specifiche misure di sicurezza previste dall'SCNTT), che le persone autorizzate abbiano accesso ai dati raccolti dal sistema di videosorveglianza [EVENTUALE] (e dal sistema di lettura targhe) - secondo livelli di visibilità differenziati in funzione della necessità di accedere ai dati personali strettamente necessari in base al ruolo posseduto - mediante il rilascio di credenziali di autenticazione individuali (anche adottando adeguate politiche di gestione delle password, nonché idonei meccanismi di *enforcement* dei requisiti ivi definiti nelle procedure di password policy);

- 7) garantire che sia possibile verificare e stabilire quali dati sono stati trattati dal sistema di videosorveglianza [EVENTUALE] (*e dal sistema di lettura targhe*), e quando, da chi e per quale scopo essi sono stati trattati (procedure di raccolta e analisi dei log);
- 8) impedire, anche mediante meccanismi di crittografia, che i dati durante il trasferimento su rete telematica, siano letti, copiati, modificati o cancellati senza autorizzazione;
- 9) garantire che, in caso di interruzione, i sistemi di videosorveglianza [EVENTUALE] (*e di lettura targhe*) possano essere riattivati attraverso idonee procedure di backup (copie di sicurezza opportunamente crittografate e conservate in modo sicuro), allo scopo di assicurarne la disponibilità, l'integrità e il recupero a seguito di un evento avverso (danneggiamento ovvero a causa di un malfunzionamento);
- 10) garantire l'affidabilità, accertandosi che eventuali anomalie nel funzionamento del sistema di videosorveglianza [EVENTUALE] (*e di lettura targhe*), siano adeguatamente segnalate;
- 11) monitorare l'efficacia delle sopra citate misure di sicurezza garantendone l'osservanza.

Sezione II – Misure di sicurezza e adempimenti a cura dell'Arma dei Carabinieri [e delle altre Forze di Polizia aderenti]

(quali Titolari autonomi del trattamento limitatamente alle operazioni di accesso logico, visualizzazione in tempo reale e differita ed estrazione investigativa delle immagini)

NOTA DI COORDINAMENTO TECNICO > Le misure organizzative, logistiche e procedurali dettagliate nella presente Sezione sono mutate dalla Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa ai sistemi di videosorveglianza urbana dell'Arma dei Carabinieri. Trattandosi di rigorosi standard minimi e di parametri ordinari di sicurezza informatica e fisica, tali misure si intendono verosimilmente applicabili anche dalle altre Forze di Polizia eventualmente aderenti.

L'Arma dei Carabinieri [e le altre Forze di Polizia aderenti], in relazione alle soluzioni tecnologiche in uso presso le proprie articolazioni per la consultazione e l'analisi dei dati messi a disposizione dal Comune, adotta le misure volte a:

- 1) installare le postazioni PC client e i monitor dedicati alla visualizzazione delle immagini di videosorveglianza esclusivamente all'interno della Centrale Operativa del Comando Provinciale/Compagnia [*e/o, in caso di adesione, delle Sale/Centrali Operative della Questura e del Comando Provinciale della Guardia di Finanza*], configurando tali ambienti come aree protette, vigilate e presidiate h24, con accesso tassativamente vietato al pubblico o a personale non addetto ai servizi info-operativi;
- 2) orientare e posizionare i monitor di controllo all'interno della Centrale Operativa in modo da non essere visibili dall'esterno dei locali o da soggetti terzi temporaneamente ammessi o in transito negli uffici;
- 3) alloggiare lo switch di rete e le terminazioni della linea telematica dedicati forniti in comodato d'uso dal Comune all'interno di armadi rack blindati, chiusi a chiave e posizionati nei vani tecnici attigui alla Centrale Operativa, neutralizzando il rischio di manomissioni o collegamenti abusivi di dispositivi esterni;
- 4) osservare l'assoluto e tassativo divieto di porre in essere qualsiasi collegamento telematico, logico o fisico tra la postazione PC client dedicata alla VDS urbana e la rete interna istituzionale dell'Arma dei Carabinieri [*o le reti Intranet della Polizia di Stato e della Guardia di Finanza*], garantendo il totale isolamento sistemico per azzerare il rischio di propagazione di minacce informatiche esterne;
- 5) impedire categoricamente l'accesso ai flussi video e alle immagini tramite tablet, smartphone, computer portatili o qualsiasi dispositivo mobile di servizio, confinando il trattamento alle sole postazioni fisse standalone debitamente autorizzate;

- 6) vietare l'utilizzo di qualsiasi dispositivo informatico o supporto di memoria di proprietà privata all'interno dell'ambiente di trattamento;
- 7) restringere l'accesso al sistema ai soli operatori espressamente autorizzati per iscritto dal rispettivo Comandante di Reparto, mediante un atto di formale nomina che definisca analiticamente i livelli di visibilità (es. solo visione live per pronto intervento o abilitazione al playback per il personale di Polizia Giudiziaria);
- 8) custodire e associare in via esclusiva, nominativa e individuale ogni singola chiave di accesso al rispettivo operatore, partendo dal presupposto che il portale rilascia le credenziali in forma anonima per preservare l'indipendenza e la riservatezza delle attività di polizia rispetto a monitoraggi esterni;
- 9) disporre la revoca immediata dei profili d'accesso e delle relative credenziali locali all'atto del trasferimento, della riorganizzazione o del congedo del dipendente;
- 10) memorizzare le sequenze video estratte per finalità di Polizia Giudiziaria (entro i 7 giorni di persistenza del dato sul server del Comune) esclusivamente su supporti rimovibili d'istituto (chiavette USB o hard disk esterni) dotati di cifratura obbligatoria;
- 11) conservare sotto chiave i supporti temporanei contenenti le evidenze probatorie all'interno degli armadi rack blindati della Centrale Operativa, procedendo all'immediata cancellazione sicura e definitiva di ogni file temporaneo locale una volta esaurite le finalità d'indagine o formalizzato il deposito presso la competente Procura della Repubblica;
- 12) sottoporre a formattazione sicura i dischi rigidi interni prima della riconsegna o sostituzione dei PC client ricevuti in comodato, provvedendo altresì a distruggere fisicamente tramite distruggidocumenti con classe di sicurezza adeguata presso il Reparto i supporti USB deteriorati o le stampe di verbali/log obsoleti;
- 13) consentire al personale tecnico del Comune o delle ditte private incaricate della manutenzione l'accesso ai locali della Centrale Operativa per interventi sui terminali o sulle linee in comodato solo ed esclusivamente previa autorizzazione del Comandante del Reparto e sotto la costante vigilanza fisica e la supervisione dei militari/operatori di servizio;
- 14) garantire un livello di sicurezza adeguato al rischio, ai sensi degli artt. 21 e 25 del D.Lgs. 51/2018, richiamato nella valutazione d'impatto dell'Arma.

CARATTERISTICHE TECNICHE DEL SISTEMA DI VIDEOSORVEGLIANZA
(ai sensi dell'art. 7, comma 1, del presente protocollo)

**ELENCO DEGLI EVENTI E DELLE SITUAZIONI
RILEVANTI PER L'ACCESSO DA PARTE DELLA CENTRALE OPERATIVA
DELL'ARMA DEI CARABINIERI [EVENTUALE] E DELLA POLIZIA DI STATO
(ai sensi dell'art. 9, comma 2, del presente protocollo)**

- A. Il personale della Centrale Operativa del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) [EVENTUALE] (*e il personale della Sala Operativa della Questura o altro ufficio periferico della Polizia di Stato*) è autorizzato ad accedere alle telecamere e visionare le immagini in tempo reale (live), per le finalità di cui all'articolo 3, comma 4, del presente protocollo operativo, in presenza degli eventi o delle situazioni qui di seguito riportate:
- 1) manifestazioni pubbliche, anche se non preavvisate;
 - 2) manifestazioni sportive;
 - 3) eventi che si svolgono in luogo pubblico che richiamano un significativo afflusso di persone;
 - 4) esecuzione di servizi di ordine e sicurezza pubblica disposti dal Questore con ordinanza di cui all'articolo 37 del decreto del Presidente della Repubblica 28 ottobre 1985, n. 782;
 - 5) esecuzione di servizi coordinati di controllo del territorio, disposti dal Questore o dal Comandante Provinciale dell'Arma dei Carabinieri;
 - 6) servizi di controllo delle infrastrutture del trasporto pubblico urbano, ferroviario, dei porti e degli aeroporti e delle aree ad esse limitrofe;
 - 7) situazioni oggetto di richieste di intervento urgente pervenute al Numero Unico di Emergenza europeo 112 (NUE 112) e smistate alla Centrale Operativa del Comando Provinciale dell'Arma dei Carabinieri (*o altra articolazione territoriale dipendente*) [EVENTUALE] (*ovvero alla Sala/Centrale Operativa della Questura o altro ufficio periferico della Polizia di Stato*), ovvero ad altri numeri di emergenza nelle Regioni in cui il NUE 112 non è stato ancora attivato;
- 8) svolgimento di operazioni di polizia giudiziaria.
- B. Il personale della Centrale Operativa del Comando Provinciale dell'Arma dei Carabinieri (*o altra articolazione territoriale dipendente*) [EVENTUALE] (*e il personale della Sala Operativa della Questura o altro ufficio periferico della Polizia di Stato*) è altresì autorizzato ad accedere alle telecamere e visionare le immagini in tempo reale (live), riprese da telecamere del sistema di videosorveglianza comunale, situate in determinate aree urbane, laddove il Prefetto - quale Autorità provinciale di pubblica sicurezza e in logica attuazione del "Patto per l'attuazione della sicurezza urbana" richiamato in premessa - abbia preventivamente provveduto ad individuarle con propria autonoma direttiva, adottata sul parere del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica (CPOSP).
- In tali casi, le Parti firmatarie danno atto che le modalità, l'arco temporale e le eventuali proroghe di tale accesso rimarranno rigorosamente subordinate a quanto stabilito all'interno del menzionato provvedimento prefettizio.

**[EVENTUALE] ELENCO DEGLI EVENTI E DELLE SITUAZIONI
RILEVANTI PER L'ACCESSO DA PARTE DELLE SALE O CENTRALI OPERATIVE
DELLA GUARDIA DI FINANZA**

(ai sensi dell'art. 9, comma 3, del presente protocollo)

- A. Il personale delle sale o centrali operative del Comando Provinciale del Corpo della Guardia di Finanza (*o altra articolazione territoriale dipendente*) è autorizzato ad accedere alle telecamere e visionare le immagini in tempo reale (live), per le finalità di cui all'art. 3, comma 4, del presente Patto (o protocollo d'intesa), limitatamente alle attribuzioni del medesimo Corpo della Guardia di Finanza, in presenza degli eventi o delle situazioni qui di seguito riportate:
- 1) manifestazioni sportive;
 - 2) pubblici spettacoli e trattenimenti;
 - 3) eventi che si svolgono in luogo pubblico che richiamano un significativo afflusso di persone;
 - 4) svolgimento di fiere e mercati su aree pubbliche;
 - 5) specifici servizi di controllo delle infrastrutture del trasporto pubblico urbano, ferroviario, dei porti e degli aeroporti e delle aree ad esse limitrofe;
 - 6) esecuzione di servizi di ordine e sicurezza pubblica disposti dal Questore con ordinanza di cui all'articolo 37 del decreto del Presidente della Repubblica 28 ottobre 1985, n. 782;
 - 7) specifici servizi di controllo delle aree in cui sono concentrati snodi organizzativi e di smistamento delle reti di distribuzione della merce illegale (contraffatta e/o pericolosa), nell'ambito di opifici, fabbriche ovvero aree industriali, artigianali e commerciali;
 - 8) specifici servizi di controllo eseguiti lungo aree urbane ed extraurbane di particolare interesse per i flussi commerciali, anche per la prossimità a zone industriali e poli produttivi;
 - 9) situazioni oggetto di richieste di intervento urgente pervenute al numero di pubblica utilità "117";
 - 10) svolgimento di operazioni di polizia giudiziaria.
- B. Il personale della Sala Operativa del Comando Provinciale della Guardia di Finanza (*o altra articolazione territoriale dipendente*) è altresì autorizzato ad accedere alle telecamere e visionare le immagini in tempo reale (live), riprese da telecamere del sistema di videosorveglianza comunale, situate in determinate aree urbane, laddove il Prefetto - quale Autorità provinciale di pubblica sicurezza e in logica attuazione del "Patto per l'attuazione della sicurezza urbana" richiamato in premessa - abbia preventivamente provveduto ad individuarle con propria autonoma direttiva, adottata sulla base del parere espresso dal Comitato Provinciale per l'Ordine e la Sicurezza Pubblica (CPOSP). Tale accesso è circoscritto alle esclusive finalità di cui all'articolo 3, comma 4, del presente protocollo operativo e limitatamente alle attribuzioni del medesimo Corpo della Guardia di Finanza, in ragione di esigenze di prevenzione e repressione della contraffazione e falsificazione dei prodotti, nonché per la prevenzione di altri fenomeni illeciti suscettibili di determinare turbative del libero utilizzo degli spazi pubblici. In tali ipotesi, le Parti firmatarie danno formalmente atto che le modalità operative, l'arco temporale di abilitazione alla visione e le eventuali proroghe dell'accesso in tempo reale rimarranno rigorosamente subordinate a quanto autonomamente determinato e disposto all'interno del menzionato provvedimento prefettizio.