COMUNE DI PISA

Tipo Atto : PROVVEDIMENTO DIRIGENTE	
N. Atto 2060	**del 10/12/2025**

Proponente : PM - Comandante

OGGETTO	**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) DEI SISTEMI DI VIDEOSORVEGLIANZA IN USO AL COMUNE DI PISA**

Uffici Partecipati	
PO SUPPORTO AL SEGRETARIO GENERALE	

IL COMANDANTE DELLA PM E SU

VISTE:

- la Deliberazione del C.C. n. 59 del 10.12.2024 con la quale è stato approvato il Bilancio di previsione 2025-2027;
- la Deliberazione della G.C. n. 344 del 23.12.2024 con la quale è stata approvata la Parte finanziaria del P.E.G. 2025-2027;
- le deliberazioni di Giunta Comunale n. 223 del 25.09.2023, n. 55 del 19.03.2024 e n. 43 del 06.03.2025 con le quali sono stati approvati l'organigramma e il funzionigramma dell'Ente;

VISTO il decreto del Sindaco n.114 del 10/11/2025 con cui è stato conferito al sottoscritto l'incarico di Elevata Qualificazione dell'Ufficio autonomo di rilevante complessità denominato *Ufficio del Comandante della Polizia Municipale e Sicurezza Urbana*, istituito, ai sensi degli artt. 23 bis, 26 e 28 del Regolamento sull'assetto organizzativo e gestionale del Comune di Pisa, approvato con la deliberazione di G.C. n.180 del 01/08/2023;

VISTO il Regolamento Generale sulla Protezione dei Dati, Regolamento UE/2016/679 (*General Data Protection Regulation* o GDPR) relativo alla p*rotezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati* di seguito indicato come GDPR, che ha abrogato la direttiva 95/46/CE ed è diventato pienamente efficace in tutti gli Stati membri dal 25 maggio 2018;

RILEVATO che:

• il GDPR è basato sul principio di *accountability* (responsabilizzazione) in virtù del quale il Titolare del trattamento adotta politiche e attua misure adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali effettuato è conforme al GDPR;

• l'articolo 35 del GDPR stabilisce, in particolare, che il Titolare del trattamento è tenuto ad effettuare una **valutazione di impatto c.d. DPIA (*Data Protection Impact Assesment*)** quando un trattamento, allorché prevede 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;

• ai sensi del GDPR la valutazione d'impatto sulla protezione dei dati è, pertanto, uno strumento importante di *accountability* in quanto permette di valutare e dimostrare il rispetto dei requisiti del trattamento come previsti dal Regolamento attraverso un processo inteso a: rappresentare le caratteristiche del trattamento dei dati personali; valutare la necessità e la proporzionalità del trattamento; valutare i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento, individuando le misure per affrontarli;

• l'art. 35 comma 3 prevede che la valutazione di impatto è richiesta, tra l'altro, nei casi di sorveglianza sistematica, su larga scala, di una zona accessibile al pubblico come nel caso di trattamento di dati personali effettuato tramite sistemi di videosorveglianza

DATO ATTO che la responsabilità della DPIA spetta al Titolare del Trattamento, che può affidare la sua conduzione materiale ad altro soggetto, interno o esterno all'organizzazione del Titolare, come indicato nelle linee guida del Garante privacy WP29

VISTO il D.Lgs 196/2003, recante "*Codice in materia di protezione dei dati personali*, come integrato dal D.Lgs 101/2018 per adeguarlo al GDPR;

RICHIAMATA la delibera di G.C. n 47 del 04/04/2019 che, ai sensi dell'art. 2-*quaterdecies,* del D.lgs. 196/2003 ha definito l'organigramma *privacy* dell'Ente e individuato ruoli, compiti e responsabilità del sistema di gestione della protezione dati nel Comune di Pisa, attribuendo ai

Dirigenti, responsabili dei servizi, il ruolo di Designati al trattamento dei dati trattati nell'ambito dei procedimenti di competenza della/e Direzione/i di cui sono responsabili;

CONSIDERATO che, secondo quanto previsto nel decreto di conferimento dell'incarico sopra richiamato, in conformità all'art. 31, comma 8, del *Regolamento sull'assetto organizzativo e gestionale* sopra richiamati, spettano al sottoscritto **tutti i compiti gestionali e operativi pertinenti all'incarico e la competenza all'adozione di tutti i provvedimenti relativi alla funzione, anche aventi rilevanza esterna, fatta eccezione di quelli di carattere dirigenziale non delegabili;**

RITENUTO quindi che **l'incarico attribuito** al sottoscritto **ricomprenda** il ruolo di Designato al Trattamento dei dati personali trattati nell'ambito dei procedimenti di competenza dell'Ufficio autonomo di rilevante complessità denominato *Ufficio del Comandante della Polizia Municipale e Sicurezza Urbana*, come risultanti dal Registro dei trattamenti approvato ogni anno dal Segretario generale, **tra i quali rientrano quelli derivanti dall'utilizzo dei sistemi di videosorveglianza del Comune di Pisa**;

DATO ATTO che, in attuazione dell'art. 35 del GDPR, il sottoscritto Comandante della Polizia Municipale e sicurezza urbana del Comune di Pisa ha rilevato la necessità di avviare un'analisi di impatto sulla protezione dati personali del sistema di videosorveglianza comunale, al fine di valutare il rispetto dei principi in materia, i rischi connessi e le eventuali misure idonee ad affrontarli;
TENUTO CONTO che per la elaborazione della presente DPIA:
- sono state coinvolte, in modo continuativo, le strutture interne ed esterne del Comune che, per le loro finalità di legge, sono interessate nel trattamento di videosorveglianza,
- è stato costantemente consultato il Responsabile della protezione dei dati (RPD) del Comune di Pisa, designato con decisione del Sindaco nr. 42 del 1 luglio 2020;
- è stato affidato altresì, ad un professionista esterno qualificato, un servizio di supporto strategico, finalizzato a coadiuvare tutti i soggetti sopra identificati nel censimento e inquadramento degli impianti di videosorveglianza in uso all'Ente, nell'adozione degli adempimenti *privacy* richiesti dalla legge; nella valutazione del rischio e nella stesura della DPIA stessa;
VISTA la **VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) DEI SISTEMI DI VIDEOSORVEGLIANZA IN USO AL COMUNE DI PISA** redatta dal sottoscritto, con il supporto del RPD e il coinvolgimento di tutti i soggetti sopra indicati;
RITENUTO che la Valutazione d'impatto sulla protezione dei dati (DPIA) dei sistemi di videosorveglianza in uso al Comune di Pisa, descrivendo la configurazione dell'architettura del sistema informatico di videosorveglianza comunale e indicando nel dettaglio le relative misure di sicurezza non possa essere resa pubblica in versione integrale, né all'albo pretorio né sulla rete civica comunale, è debba essere parzialmente esclusa dal diritto di accesso per ragioni di sicurezza informatica, potendone essere pubblicato solo un estratto, allegato alla presente, quale parte integrante e sostanziale, come **doc.1**;
DATO ATTO che, come risulta dalle conclusioni dell'estratto allegato come doc.1, l'esito della stessa è POSITIVO in quanto, a seguito dell'individuazione e attuazione delle misure organizzative e di sicurezza in essa descritte, allo stato attuale, i dati personali relativi all'insieme dei trattamenti in esame sono:

trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

raccolti per finalità determinate, esplicite e legittime;

adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

esatti e aggiornati («esattezza»);

conservati in una forma che consente l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti;

trattati in maniera da garantire un'adeguata sicurezza e protezione dei dati personali, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

DATO ATTO che la DPIA rappresenta uno strumento di valutazione dinamico, soggetto a riesame ogni qualvolta si modifichi il quadro dei rischi derivati dai trattamenti;

PRESO ATTO altresì del parere positivo, richiesto ai sensi dell'art. 39, par. 1, lett c) del GDPR, espresso in calce alla DPIA dal RPD dell'Ente

RITENUTA la propria competenza per materia all'adozione del presente provvedimento, non rientrando tra quelli di carattere dirigenziale non delegabili elencati all'art. 34, comma 4 del *Regolamento sull'assetto organizzativo e gestionale* di cui sopra;

VISTO il Regolamento Comunale per l'utilizzo della videosorveglianza, approvato con deliberazione del C.C. nr. 7 del 23/02/20212;

VISTI altresì:

il D.Lgs. 267/2000; la Lg 241/1990;

le Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;

DETERMINA

1. **di approvare** la **VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEI SISTEMI DI VIDEOSORVEGLIANZA IN USO AL COMUNE DI PISA** redatta, ai sensi dell'art. 35 del Regolamento (UE) n.679/2016, ed i relativi allegati;
2. **di stabilire** che, per le ragioni di sicurezza espresse in narrativa, la stessa resta conservata in atti d'ufficio e sarà formalizzata con protocollo interno riservato, per essere consultabile ed esibibile in caso di controlli dell'Autorità;
3. **di disporre** la pubblicazione all'albo pretorio e, per il tramite del RPD, nella pagina **Protezione dati** del sito web istituzionale dell'**estratto della DPIA**, allegato alla presente come **doc.1**
4. **di partecipare, con protocollo interno riservato,** la VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEI SISTEMI DI VIDEOSORVEGLIANZA IN USO AL COMUNE DI PISA, in versione integrale, al Sindaco *pro-tempore*.

Il COMANDANTE
DELLA POLIZIA MUNICIPALE
E SICUREZZA URBANA
Dott. Gionata Gualdi

Documento firmato digitalmente da

GIONATA GUALDI / ArubaPEC S.p.A.

COMUNE DI PISA

TITOLARE DEL TRATTAMENTO DATI

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI DEI SISTEMI DI VIDEOSORVEGLIANZA IN USO AL COMUNE DI PISA

DPIA
(*DATA PROTECTION IMPACT ASSESSMENT*)

ESTRATTO PER PUBBLICAZIONE

ART. 35 REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DI DATI PERSONAL

ART. 23 DEL D.LGS N. 51 DEL 18/05/18 RELATIVO ALL'ATTUAZIONE DELLA DIRETTIVA UE 2016/680 IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELLE AUTORITÀ COMPETENTI

Adottata con determina n. del
Rev.1:
Rev.2:

Sommario

1 L'obbligatorietà della valutazione d'impatto per i trattamenti dei dati personali raccolti dai sistemi di videosorveglianza.

Tra le materie di competenza di una Amministrazione Pubblica Locale la sicurezza urbana rappresenta uno dei compiti più gravosi e delicati perché la domanda di sicurezza dei cittadini è fortemente aumentata e, a questo fine, sono stati notevolmente accresciuti i compiti assegnati al Sindaco e alle forze di Polizia Locale, di concerto con quella nazionale

Con il Decreto del Ministro dell'Interno del 5 agosto 2008, che ha definito la *sicurezza urbana come quel bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale*, infatti troviamo attribuito ai Sindaci, attraverso l'utilizzo della Polizia Locale o altri idonei strumenti, l'intervento e l'adozione di misure atte a prevenire e contrastare:

- situazioni di degrado favorite dall'insorgere di fenomeni criminosi;
- spaccio di stupefacenti;
- sfruttamento della prostituzione;
- fenomeni che facilitano l'immigrazione clandestina;
- fenomeni di violenza legati anche all'abuso di alcool;
- danneggiamento al patrimonio pubblico e privato;
- accattonaggio molesto;
- comportamenti che possano offendere la pubblica decenza ovvero turbino gravemente il libero utilizzo degli spazi pubblici;
- eventuale intralcio alla pubblica viabilità o l'alterazione del decoro urbano;
- abusivismo commerciale;
- illecita occupazione di suolo pubblico;
- deposito illecito di rifiuti.

In questo ambito la funzione svolta dai sistemi di videosorveglianza a supporto della sicurezza urbana è indiscutibile, soddisfacendo l'esigenza di maggiori garanzie per la sicurezza, e pienamente riconosciuta dal legislatore. Ai sensi dell'art. 6 del d. lg 23 febbraio 2009, n. 11, convertito nella legge 23 aprile 2009, n. 38, per la tutela della sicurezza urbana i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico. L'utilizzo della videosorveglianza, infatti, garantisce un valido supporto nelle indagini e, allo stesso tempo, rappresenta un ottimo strumento dissuasivo e deterrente alla commissione di reati e illeciti amministrativi.

La videosorveglianza però, seppur funzionale a prevenire e contrastare fenomeni di criminalità ed a garantire sicurezza urbana, vivibilità e decoro delle città, va gestita nel rispetto dei diritti e delle libertà fondamentali dei cittadini ed, in particolare, del loro diritto alla protezione dei dati personali, rispetto ai quali i sistemi di videosorveglianza possono rivelarsi molto invasivi.

Le immagini, ovvero i dati personali delle persone fisiche, raccolti tramite tali sistemi devono essere trattati in conformità alla normativa vigente secondo il principio di "*accountability*" ovvero di "*responsabilizzazione*" (art. 24 del GDPR) del Titolare del Trattamento, a cui compete l'adozione di tutte le misure di sicurezza, tecniche ed organizzative, necessarie ad assicurare adeguata protezione a tali dati personali. L'*accountability* del Titolare impone:

COMPLIANCE ovvero garanzia che il trattamento avvenga nel rispetto delle norme e che l'azione pubblica sia mantenuta nell'alveo tracciato dalle leggi;
TRASPARENZA ovvero accessibilità alle informazioni per i cittadini.

RESPONSIVITÁ ovvero capacità di rendere conto di scelte, comportamenti e azioni e quindi. *DOCUMENTABILITA'* degli adempimenti richiesti dal GDPR, nel senso che il Titolare non solo deve adottare, ma deve anche essere in grado di dimostrare di aver adottato, tutte le misure di sicurezza tecniche ed organizzative necessarie ad assicurare adeguata protezione ai dati personali trattati nell'esercizio dei propri compiti istituzionali.

La normativa di riferimento in materia di videosorveglianza è costituita da:

- Regolamento UE 679/2016, c.d. GDPR (*General Data Protection Regulation*), obbligatorio per tutti gli Stati membri dell'UE e direttamente operante in Italia a partire dal 25 Maggio 2018;
- Direttiva UE 680/2016 c.d. Direttiva Polizia e relativo decreto di recepimento (D.Lgs 51/2018),
- D.lgs 196/2003 "*Codice in materia di protezione dei dati personali*" come novellato dal D.Lgs 101/2018,
- Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali ed in particolare il Provvedimento Generale in materia di videosorveglianza dell'8 aprile 2010 sempre applicabile per le parti non incompatibili;
- Regolamento sull'utilizzo del sistema di videosorveglianza, approvato dall'Ente con delibera C.C. n.7 del 23/02/2012 e in fase di revisione.

In particolare l'art. 35, primo capoverso, del GDPR (art. 23, comma 1, del D.Lgs 51/2018) stabilisce che *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 una "*valutazione del suo impatto sulla protezione dei dati personali*". Il legislatore comunitario prosegue elencando i casi in cui tale valutazione è da considerarsi obbligatoria prevedendo, all'art. 35, terzo capoverso, lett c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.* La **Valutazione d'impatto sulla Protezione Dati**, c.d. DPIA *(Data Protection Impact Assessement*) altro non è che una **procedura che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità, nonché i relativi rischi allo scopo di approntare misure idonee ad affrontarli.** Essa contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure di sicurezza e i meccanismi adottati per contenere tali rischi ed assicurare che il trattamento dei dati avvenga nel rispetto delle norme tese ad assicurare a tali dati adeguata protezione.

Il Comune di Pisa è dotato di un sistema di videosorveglianza per finalità di sicurezza urbana integrata, installato dall'Amministrazione Comunale con possibilità di trattamento autonomo dei dati raccolti da parte di altre Forze di Polizia, in attuazione del d.lg. 14/2017, convertito nella Lg n. 48/2017 (vd. par. 2). Tale sistema è utilizzato anche per la prevenzione dell'ordine e sicurezza pubblica per quanto di competenza, per la prevenzione o repressione dei reati o esecuzione di sanzioni penali, per attività di polizia e/o istituzionali. L'Ente si avvale anche di sistemi di videosorveglianza per la repressione degli illeciti in materia ambientale, per la tutela della sicurezza e incolumità degli operatori di Polizia, per la tutela del proprio patrimonio e per garantire sicurezza nei luoghi di lavoro.

La presente DPIA prende in considerazione il trattamento, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo dei sistemi di videosorveglianza di cui è dotato il Comune di Pisa per verificare che l'Ente assicuri ad essi adeguata protezione in conformità al GDPR. La DPIA è stata redatta alla luce del principio della "*privacy by design e privacy by default*" (art 25 del GDPR) ovvero valutando che il trattamento dati, sin dalla progettazione (*by design*) e per impostazione predefinita, quindi al momento della configurazione e implementazione dei mezzi di trattamento (*by default*), sia condotto in conformità ai principi di protezione dati e alla normativa di riferimento applicabile

Per la redazione della presente DPIA il Comune di Pisa, nella sua qualità di Titolare del trattamento, si è avvalso della collaborazione dei vari soggetti coinvolti quali il Comandante della Polizia Municipale e Sicurezza Urbana, Designato al trattamento dei dati personali derivanti dall'utilizzo dei sistemi di videosorveglianza, i Responsabili esterni del trattamento, ovvero i fornitori esterni che trattano dati per conto del Titolare in ragione di un contratto di manutenzione dei sistemi, i Dirigenti o Funzionari amministrativi, tecnici ed informatici dell'ente, di volta in volta e per quanto di loro competenza, coinvolti nel trattamento dei dati ed il Responsabile della Protezione Dati (di seguito RPD), che ha svolto un ruolo di supporto giuridico e coordinamento.
Il Comune di Pisa ha affidato anche un professionista esterno qualificato un servizio di supporto strategico, finalizzato a coadiuvare i soggetti sopra identificati nel censimento e inquadramento degli impianti di videosorveglianza e geo localizzazione in uso all'Ente, nell'adozione degli adempimenti privacy richiesti dalla legge per la videosorveglianza; nella valutazione del rischio; nella redazione delle convenzioni operative e nella stesura della presente DPIA.

2. La Sicurezza Urbana Integrata nel Comune di Pisa. Il Patto Sicurezza Pisa 2018.

Con il Decreto Legge 20 febbraio 2017, n. 14, convertito con modificazioni dalla Legge 18 aprile 2017, n. 48, meglio noto come "***Pacchetto sicurezza Minniti***", è stato riformulato il concetto di sicurezza urbana definita, all' art. 4, come *il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità (in particolare di tipo predatorio)* ***da potenziare con accordi/patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza*** e sono state individuate le direttrici d'azione che Stato ed Enti Locali devono sviluppare con riguardo alle rispettive competenze.
Con il p*atto per la sicurezza urbana* (ex art. 5 del decreto legge n. 14/2017, convertito con modificazioni dalla legge 18 aprile 2017, n. 48) sottoscritto tra il Comune e la locale Prefettura (allegato alla presente sotto la lettera **Q – "PATTO PER PISA SICURA"**, la Prefettura e il Comune di Pisa, nel rispetto delle reciproche competenze, hanno adottato strategie congiunte, volte a migliorare la percezione di sicurezza dei cittadini e a contrastare ogni forma di illegalità. L'attuazione delle finalità e degli strumenti sopra individuati è avvenuto anche attraverso un progetto, integrato, di sistemi di videosorveglianza, elaborato nel rispetto delle disposizioni dell'Autorità Garante per il trattamento dei dati personali, che è stato valutato, quanto alle modalità di impiego e ad ogni aspetto tecnico operativo, in coerenza con le direttive ministeriali emanate in materia, in particolare con la circolare del Ministero dell'Interno 558/SICPART/421.2/70/224632 del 2 marzo 2012, recante "*Sistemi di videosorveglianza in ambito comunale. Direttiva*" e agli atti ivi richiamati. Il sistema opera anche il monitoraggio automatico delle targhe auto (ALPR = *Automatic License Plate Recognition*) nei principali varchi di accesso. Per la descrizione del suddetto sistema di videosorveglianza si rinvia ai paragrafi 5.2.1. e 5.2.2.
Circa i "ruoli *privacy*" in caso di videosorveglianza urbana integrata, il Garante per la protezione dei dati personali, nel proprio Provvedimento n. 1712680 dell'8 aprile 2010, ha riconosciuto che Titolari autonomi del trattamento possano utilizzare le medesime infrastrutture tecnologiche senza troppe formalità. Oggi, le Linee Guida 7/2020 "*Linee guida sui concetti di Titolare e responsabile nel GDPR*", approvate dal Comitato Europeo per la Protezione dei Dati, di seguito EDPB (*European Data Protection Board*) il 7 luglio 2021, confermano questa possibilità di utilizzo condiviso della medesima infrastruttura tecnologica da parte di Titolari autonomi, quali Comuni e Forze di polizia dello Stato (paragrafi 68 e 71). Per formalizzare quest'attività interforze, sarebbe auspicabile la sottoscrizione di uno specifico accordo tra autonomi Titolari, secondo la bozza che si allega alla presente sotto la lettera **N – ACCORDO TITOLARITA' AUTONOMA** da cui si evinca che il

Comune persegue le finalità di sicurezza urbana con i propri strumenti di videosorveglianza in qualità di Titolare autonomo, mentre la Prefettura, dal canto suo, persegue finalità di ordine e sicurezza pubblica, da raggiungere anche tramite l'utilizzo del sistema di videosorveglianza comunale, accordo che qualifichi il Comune come gestore dell' impianto di videosorveglianza interforze, cui accede in sicurezza ed autonomia, anche la Prefettura (e quindi tutte le forze di polizia dello Stato), Titolari autonomi (ma con finalità convergenti), per lo svolgimento delle proprie attività.
Nelle more della sottoscrizione del suddetto accordo tra autonomi Titolari, l'accesso delle forze di Polizia dello Stato trova la propria base giuridica, che legittima il trattamento, nello specifico Patto per Pisa sicura sopra ricordato.

3. Normative Speciali – Applicazioni nel Comune di Pisa

Quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive o richiesta per la sicurezza del lavoratori ci troviamo sempre nella situazione di dover coniugare:

- gli obblighi, imposti al datore di lavoro, di evitare o ridurre al minimo l'esposizione dei lavoratori a rischi legati all'attività lavorativa e tutelare l'integrità fisica e la personalità morale dei lavoratori (D.lgs 81/2008 *Testo Unico in materia di salute e sicurezza nei luoghi di lavoro*) con
- le garanzie previste in materia dallo Statuto dei lavoratori e
- le garanzie dei tutela ed esercizio dei diritti da parte degli interessati dal trattamento dei dati previste dal GDPR e dal Codice in materia di protezione dei dati personali

3.1 Videosorveglianza per sicurezza dei luoghi di lavoro – L. 300/1970 "Statuto dei Lavoratori"

L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori costituisce reato, così come stabilito anche all'art. 171 del Codice Privacy (d.lgs. 196/2003) a seguito delle modifiche operate dal d.lgs. 101/2018, in applicazione del GDPR. Nel caso in cui la videosorveglianza sia installata per esigenze organizzative o produttive, ovvero per ragioni di tutela del proprio patrimonio e per garantire sicurezza sui luoghi di lavoro, se, anche solo incidentalmente, può comportare un controllo a distanza dei lavoratori, deve essere accompagnata da una serie di cautele imposte dallo Statuto dei lavoratori.
L´art. 4 della l. n. 300/1970, stabilisce infatti che gli impianti e le apparecchiature "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con organizzazioni sindacali di rappresentanza, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti*".
Presso il Comune di Pisa risultano presenti telecamere fisse di contesto, installate a tutela del patrimonio e a garanzia della sicurezza dei luoghi di lavoro, che, insistendo appunto sui luoghi di lavoro, possono incidentalmente riprendere i lavoratori all'interno dei luoghi di lavoro o loro pertinenze, introducendo il rischio di attuare forme di controllo sulle attività lavorative.
Tali impianti di videosorveglianza, indipendenti dal sistema di videosorveglianza urbana, sono composti da telecamere ad orientamento fisso o brandeggiabile, insistenti sul perimetro o sull'interno di edifici pubblici volte ad assicurare sicurezza e tutela dell'incolumità dei dipendenti ed operatori di Polizia Locale, tenuta in sicurezza delle armi di cui questa è dotata, nonché tutela del patrimonio pubblico immobiliare (ingressi di edifici pubblici) o mobiliare (autorimessa per i mezzi di proprietà dell'ente pubblico). Essi interessano:

OMISSIS
OMISSIS

Relativamente ai suddetti impianti, è necessario:

stipulare accordo sindacale con le Organizzazioni Sindacali ai sensi dell'articolo 4 della Legge 300/1970 ("Statuto dei Lavoratori"), secondo il form allegato **"D – ACCORDO SINDACALE VDS L. 300_70";**
adottare, nei confronti della ditta incaricata della manutenzione tecnica dei dispositivi mobili di ripresa, che tratta dati per conto del Titolare, atto di nomina come Responsabile esterno del trattamento ex art. 28 GDPR, secondo il *form* allegato alla presente come "**A – ATTO DI NOMINA RESPONSABILE ESTERNO**" o come "**AA – ATTO DI NOMINA DI RESPONSABILE AS**" se incaricata anche delle funzioni di amministratore di sistema e/o procedere con atto di nomina di Amministratore di Sistema, secondo il *form* allegato alla presente sotto la lettera **"B – ATTO DI NOMINA AMMINISTRATORE DI SISTEMA INTERNO"** nei confronti del personale tecnico interno all'Ente, se la funzione di gestione e manutenzione tecnica di tali impianti è svolta da personale interno
nominare, da parte del Comandante, Designato al trattamento dei dati, dipendenti di comprovata esperienza e formazione, come autorizzati al trattamento di tali, con atto secondo il *form* allegato alla presente come "**C – ATTO DI NOMINA AUTORIZZATI VDS OPERATORI DI PL**" e, nel caso invece di impianti a circuito chiuso a tutela di luoghi di lavoro o di immobili, che non siano collegati con il Comando di PL, a cura del Dirigente Designato al trattamento dei dati raccolti da quel sistema di videosorveglianza, dipendenti di comprovata esperienza e formazione, quali autorizzati al trattamento della sola visione dei monitor con atto secondo il *form* allegato alla presente come **"CC – ATTO DI NOMINA AUTORIZZATI VDS LUOGHI DI LAVORO AD PERSONAM"** laddove le telecamere prevedono la visione in tempo reale delle immagini;
stabilire un tempo di conservazione delle immagini di 72 ore, nel caso di finalità di tutela del patrimonio e luoghi di lavoro, fatte salve diverse esigenze di Polizia;
adottare apposita **Informativa di I° Livello** da apporre sul luogo di utilizzo di tali apparati, allegata alla presente come "**EE – INFORMATIVA I LIVELLO LUOGHI DI LAVORO"** contenente *Qrcode* e *link* di rinvio all'Informativa di II Livello
adottare apposita **informativa di II° livello,** pubblicata anche sul sito istituzionale dell'ente nella sezione "Protezione Dati", ed allegata alla presente come "**F - INFORMATIVA ESTESA II LIVELLO VDS"**

3.2 Dispositivi mobili di videoripresa a contrasto dell'abbandono dei rifiuti (Fototrappole)

Per il controllo delle aree utilizzate come discariche di materiali e di sostanze pericolose, in applicazione dei principi generali di liceità, finalità e proporzionalità applicabili al trattamento di dati personali, di cui all'art. 5 del GDPR, , l'utilizzo di sistemi di videosorveglianza è lecito solo se non risulti possibile o efficace il ricorso a strumenti e sistemi di controllo alternativi e appaia necessario monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689). In questo senso si è espresso il Garante per la Protezione dei dati Personali (GPDP) nel proprio Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Doc Web. n. 1712680 - Gazzetta Ufficiale n. 99 del 29 aprile 2010, punto 5.2).
Dall'analisi effettuata con la presente DPIA è emerso che il Comando della Polizia Municipale utilizza dispositivi di videoripresa mobili che, a seconda delle modalità di posizionamento e finalità di utilizzo, possono essere assimilate a c.d. "**Foto Trappole**" o telecamere di videosorveglianza per attività di controllo

dell'abbandono di rifiuti ed eventuale prevenzione e/o repressione di reati connessi (schede tecniche **allegati W e Y**). L'Amministrazione, in quanto membro dell'ATO Toscana Costa, Autorità di Ambito Territoriale Ottimale per la gestione integrata dei rifiuti nell'ATO, per contratto di servizio, si avvale di RetiAmbiente spa per la installazione, gestione, manutenzione e ripristino del sistema. RetiAmbiente è stata nominata dal Comune quale responsabile esterna del trattamento ex art. 28 del GDPR, che si avvale, a sua volta, di una ditta esterna sub-responsabile che materialmente si occupa di posizionamento, rimozione, manutenzione apparati, scarico e verifica tecnica della validità dei fotogrammi, trasmessi al personale della Polizia Municipale, formalmente nominato come autorizzato al trattamento di tali dati. Rispetto alla videosorveglianza svolta per questa finalità, il Comune Titolare ha adottato le seguenti misure di sicurezza tecniche ed organizzative:

DISCIPLINARE TECNICO DI ISTRUZIONI PER L'IMPIEGO DI SISTEMI DI VIDEOSORVEGLIANZA MOBILE E RICOLLOCABILE, approvato con determinazione n. 657 del 2 maggio 2024 del Comandante della PM e SU, allegato alla presente sotto la lettera **H**;
nomina del personale della Polizia Locale addetto al trattamento dei dati eseguiti attraverso dispositivi di video ripresa cd "mobili", con atto adottato secondo il *form* allegato sotto la lettera **"L– ATTO DI NOMINA VDS AD PERSONAM PL"** contenente le necessarie istruzioni come richieste dall'art.29 del GDPR**;**
verifica che i dispositivi di video ripresa mobile in uso utilizzino sistemi di cifratura delle immagini cd "sicuri" e tali da, in caso di rimozione di eventuali memorie asportabili (SSD, ecc) o degli stessi apparati, non consentire a soggetti non autorizzati di poter accedere e decifrare le immagini in essi contenute;
nomina a responsabile esterno del trattamento ex art. 28 GDPR della ditta incaricata della manutenzione tecnica dei dispositivi mobili di ripresa, contenente relative prescrizioni e misure di sicurezza, secondo il form allegato alla presente come **"A – ATTO DI NOMINA RESPONSABILE ESTERNO"**
previsione di un tempo di conservazione delle registrazioni, di norma, di 7 giorni, fatte salve diverse esigenze di Polizia. Solo per eventuali, necessarie e improcrastinabili attività tecniche connesse alla gestione e manutenzione degli apparati, previsione della possibilità di uno slittamento delle tempistiche di ulteriori 7 giorni naturali e consecutivi rispetto ai tempi previsti.
adozione di Informativa di I° Livello da apporre, da parte della ditta incaricata all'installazione previa indicazione del luogo di posizionamento da parte degli operatori di Polizia Locale addetti a tale trattamento dei dati, sul luogo di utilizzo di tali apparati, allegata alla presente come "**EEE – INFORMATIVA I LIVELLO VDS AMBIENTE**"
adozione di informativa di II° livello per tale trattamento, che è stata pubblicata sul sito istituzionale dell'ente comunale ed allegata alla presente come "**F - INFORMATIVA ESTESA II LIVELLO VDS"**

Poiché anche questi sistemi di VDS mobili, per la loro modalità di posizionamento, incidentalmente possono riprendere i lavoratori che operano singolarmente o in pattuglia (formata da 2 o più operatori di Polizia Locale o dagli addetti alla loro manutenzione)e quindi attuare "invasive" forme di controllo sulle loro attività lavorativa, il loro utilizzo è stato inoltre inserito nell'accordo**,** sottoscritto con le Organizzazioni Sindacali ai sensi dell'articolo 4 della Legge 300/1970 ("Statuto dei Lavoratori"), allegato parte integrante alla presente DPIA, sotto la lettera **D – ACCORDO SINDACALE VDS L. 300_70**;

3.3 Dispositivi di videoripresa Aereo Mobili (Droni)

In generale l'utilizzo dei droni per finalità di polizia ha visto negli anni una crescente produzione normativa.

Per quanto di interesse delle Forze di Polizia Locale sono da considerare in particolare:

il Regolamento Delegato (UE) 2019/945 della commissione del 12 marzo 2019, relativo ai sistemi aeromobili senza equipaggio e agli operatori di paesi terzi di sistemi aeromobili senza equipaggio.
il Regio decreto del 30 marzo 1942, n. 327, e successive modificazioni, recante "Codice della Navigazione" e, in particolare, il dettato dell'articolo 743 del Codice della Navigazione, recentemente aggiornato, dove alla nozione di aeromobile, riporta: "*Per aeromobile si intende ogni macchina destinata al trasporto per aria di persone o cose. Sono altresì considerati aeromobili i mezzi aerei a pilotaggio remoto, definiti come tali dalle leggi speciali, dai regolamenti dell'ENAC e, per quelli militari, dai decreti del Ministero della Difesa. Le distinzioni degli aeromobili, secondo le loro caratteristiche tecniche e secondo il loro impiego, sono stabilite dall'ENAC con propri regolamenti e, comunque, dalla normativa speciale in materia*" e l'articolo 746, recante disposizioni sugli aeromobili equiparabili a quelli di Stato
la Direttiva del Presidente del Consiglio dei Ministri del 23 settembre 2011, recante la disciplina del trasporto aereo di Stato;
il documento del "Gruppo di Lavoro Art. 29" e intitolato "*Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*" redatto dal "Working Party" definito sotto l'art.29 della Direttiva 95/46/EC (adottato il 16 giugno 2015)
il documento EDPS (European Data Protection Supervisor) *Opinion on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*"
i dettati degli Artt. 614 "*Violazione di domicilio*" e 615-bis "*Interferenze illecite nella vita privata*" del Codice Penale
la "*Pagina informativa sui droni ad uso civile*" dell'EASA (Agenzia Europea per la Sicurezza Aerea)

In base a quanto previsto dal GDPR (Regolamento UE 2016/679), i droni, come tutti i dispositivi elettronici, secondo il principio di *privacy by design e privacy by default,* devono essere costruiti e configurati per raccogliere meno dati personali possibile nel rispetto del principio di minimizzazione.
A questo proposito, un'attenzione particolare riveste il recentissimo **Regolamento UAS-IT,** pubblicato il 04 gennaio 2021 che, all'articolo 29, rubricato "*Protezione dei dati e privacy*", richiama esplicitamente il **principio di minimizzazione dei dati previsto dall'art. 5, paragrafo 1, lett. C del Regolamento n.679/2016** prevedendo che: *"Laddove le operazioni svolte attraverso UAS* (Unmanned aerial system ovvero Sistema Aeromobile a Pilotaggio Remoto) *possano comportare un trattamento di dati personali, tale circostanza deve essere menzionata nella documentazione sottoposta ai fini del rilascio della pertinente autorizzazione." "Il trattamento dei dati personali deve essere effettuato in ogni caso nel rispetto del Regolamento (UE) 2016/679 e del Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni ("Codice in materia di protezione dei dati personali"), con particolare riguardo al rispetto del principio di minimizzazione dei dati di cui all'articolo 5(1)(c) del predetto Regolamento*."
L'utilizzo di Droni, oltre a dover garantire il rispetto della normativa in materia di protezione dei dati personali, è lecito anche solo se attuato nel rispetto della regolamentazione emanata nel tempo dalle varie autorità nazionali o UE nonché delle regole previste dall'ENAC per far volare i Sistemi Aeromobili a Pilotaggio Remoto (www.enac.gov.it).

All'interno del Comune di Pisa i droni sono utilizzati per attività di "Rilievi fotogrammetrici" dal:

- **Settore Edilizia (**scheda tecnica **Allegato T)** per l'attività istituzionale di verifiche e riscontro di conformità in materia di edilizia pubblica e privata (eventuali abusi edilizi con relativa segnalazione alla Polizia Locale) e per adempimenti, a seguito di apposito accordo con la

Regione Toscana, derivanti dall'adesione sperimentale alla piattaforma fotogrammetrica regionale. Con tale accordo si sono regolati anche i rapporti privacy tra Comune, Titolare e Regione, Responsabile del Trattamento per la messa a disposizione della piattaforma.

Con riguardo alle suddette finalità, si rileva che di norma, i rilievi fotogrammetrici non sono attuati con definizione tale da permettere l'identificazione "diretta" o "indiretta" di eventuali soggetti involontariamente video ripresi. Sono stati comunque disciplinati con appositi atti:

le nomine da parte del Dirigente Designato al Trattamento Dirigente degli autorizzati al trattamento dei Dati, secondo il *form* allegato alla presente come "**I - ATTO DI NOMINA VDS DRONE EDILIZIA"** con relative istruzioni

l'adozione di istruzioni e prescrizioni per l'utilizzo dei Droni allegato alla presente come "**J - ATTO UTILIZZO DRONI INFORMATIVA E PRESCRIZIONI**".

informativa di I Livello, allegato alla presente come "**JJ - INFORMATIVA I LIVELLO DRONE EDILIZIA**".

informativa di II° livello che è stata pubblicata sul sito istituzionale dell'ente comunale, allegato alla presente come "**JJJ- INFORMATIVA II LIVELLO DRONE EDILIZIA**";

- **Settore Polizia Locale (allegati U e V)** per attività di polizia giudiziaria, d'iniziativa e delegata dalla Procura della Repubblica, finalizzata all'accertamento e alla repressione di illeciti penali; attività di pubblica sicurezza, ai sensi della L. 65/ 86; vigilanza sullo stato di manutenzione e conservazione di beni immobili pubblici o di interesse pubblico (strade, edifici, opere pubbliche etc.) e privati, specie in caso di minaccia all'incolumità pubblica o pericolo di crollo, anche in collaborazione con altri Settori del Comune o Enti esterni (Settore Edilizia del Comune, VV.FF, Sovrintendenza, etc); azioni di prevenzione, contrasto e repressione di abusivismo commerciale, di illeciti in materia ambientale, di illeciti in materia di stupefacenti; attività di soccorso in pubblici e privati infortuni, nonché in caso di calamità e di ricerca di persone scomparse in zone disagiate o mal raggiungibili (per la quale l'utilizzazione degli aeromobili posseduti è particolarmente efficace in ragione della particolare configurazione – "Ricerca e soccorso" – del velivolo stesso); per rilievo di sinistri stradali, monitoraggio del traffico e dei nodi critici viari; per azioni di prevenzione e contrasto al degrado urbano, anche in funzione di prevenzione e repressione di atti di devianza e criminalità urbana; per attività di *safety* e *security* in occasione di eventi pubblici (v. Circolare Ministro dell'Interno Piantedosi), per altre attività di Polizia per quanto di competenza del settore;

Il Comune di Pisa è autorizzato al suddetto utilizzo dal Ministero delle infrastrutture e dei trasporti - Direzione Generale per gli Aeroporti, il Trasporto Aereo e i Servizi Satellitari con Decreto di equiparazione ad aeromobile di Stato, ai sensi dell'articolo 746 del Codice della Navigazione, degli aeromobili della Polizia Locale di Pisa prot. 0000004 del 06.02.2023.

Solitamente non vi sono dati personali trattati. Le immagini raccolte durante il rilievo, principalmente con riprese zenitali o prossime allo zenitale, o comunque perpendicolare alla superficie che si vuole rilevare, non permettono il riconoscimento delle persone che, accidentalmente, potessero essere comunque riprese. Il software di elaborazione post processo, comunque, scarta automaticamente le immagini con soggetti in movimento (come appunto le persone, i veicoli, ed altri -animali-) rendendole irriconoscibili o non presenti nell'output di prodotto.

Sono comunque applicate le limitazioni e garanzie seguenti:

1. in ragione del GDPR le immagini saranno acquisite e trattate prioritariamente per gli scopi indicati nell'informativa;
2. le memorie di cui è fornito l'apparato A.P.R. (siano esse *built in*, oppure rimuovili) impiegate dal Comune di Pisa saranno munite di idonea cifratura tale che i dati in esse catturati ed eventualmente immagazzinati, nel rispetto delle tempistiche del progetto, non saranno comunque fruibili a terzi (protezione attiva ai fini della salvaguardia e prevenzione da eventi *data breach*);
3. in alternativa saranno dislocate fisicamente sotto il diretto controllo degli operatori e non posizionate a bordo dei velivoli;
4. l'accesso alla stazione di controllo (pad di controllo) che permette di accedere alle funzioni di pilotaggio remoto sarà criptato da password nella conoscenza del pilota addetto alla missione, così da rendere inservibile l'aeromobile ed i dati in esso eventualmente contenuti, a soggetti non autorizzati

E sono altresì stati individuati e disciplinati con appositi atti:

le nomine degli operatori autorizzati al trattamento dei dati, secondo il *form* allegato come **"L - ATTO DI NOMINA AUTORIZZATO VDS AD PERSONAM PL";**
apposite istruzioni e prescrizioni per l'utilizzo dei Droni allegate alla presente come "**J - ATTO UTILIZZO DRONI INFORMATIVA E PRESCRIZIONI**";
informativa di I Livello, allegato alla presente come "**LL - INFORMATIVA I LIVELLO DRONE PM**";
informativa di II° livello per tale trattamento che è stata pubblicata sul sito istituzionale dell'ente comunale, allegato alla presente come "**LLL-INFORMATIVA II LIVELLO DRONE PM**

3.4 Dispositivi di videoripresa indossabili "Body Cam"

La Body Cam è un dispositivo di registrazione audio, video o fotografico indossabile su vestiti, divise o caschi, che può essere impostata sia per scattare foto in tempo reale che per effettuare una registrazione continua di video.
La Polizia Locale, in occasione di eventi o manifestazioni pubbliche, anche in ausilio ad altre Forze di Polizia ad ordinamento statale, può trovarsi a dover fronteggiare complesse situazioni di ordine e sicurezza pubblica ed a contrastare condotte violente e/o di turbamento dell'ordine pubblico. A ciò possono aggiungersi altre situazioni di pericolosità, a cui gli operatori di polizia locale possono trovarsi esposti nello svolgimento di attività e compiti istituzionali come, ad esempio, quando svolgono attività di Polizia Giudiziaria attraverso sequestri, confische o arresti, che spesso provocano reazioni anche aggressive da parte dei soggetti destinatari di tali provvedimenti.
L'utilizzo di *Body Cam*, quale strumento atto a produrre prove documentali certe ed incontestabili, sia ai sensi dell'articolo 13 della della Lg 689/81 "*Modifiche al sistema penale*" che del Codice Penale, costituisce un valido deterrente contro le aggressioni agli operatori di polizia, nonché una fonte di prova documentale a tutela sia degli operatori di Polizia che dello stesso cittadino comune o fuggitivo.
Il Garante per la Protezione dei Dati personali con due distinti pareri [doc. web 9690691 e n. 9690902] ha dato via libera all'uso delle Body Cam per documentare situazioni critiche di ordine pubblico in occasione di eventi o manifestazioni, dettando però una serie di prescrizioni relativamente a misure di sicurezza e tracciamento degli accessi, necessarie a garantire che il trattamento avvenga in conformità alla normativa sulla protezione dei dati personali. Nell'utilizzo delle Body Cam, infatti i rischi per i diritti e la libertà dei soggetti ripresi possono essere indubbiamente elevati, ove si consideri che il loro utilizzo, sovente nel corso di manifestazioni pubbliche, comporta il trattamento anche di dati che rivelano opinioni politiche, sindacali, religiose ed orientamento sessuale dei partecipanti. Le suddette prescrizioni del GPDP sono state recepite dal Ministero dell'Interno nelle linee Guida sull'utilizzo delle Body Cam adottate il 18 gennaio 2022.
Dall'analisi effettuata con la presente DPIA, risultano presenti dei dispositivi di videoripresa mobili indossabili Body Cam **(**scheda tecnica **allegato S)** in uso esclusivo al personale del Comando della Polizia Municipale di

Pisa, il cui utilizzo è ammesso solo per la produzione di "prove documentali" inerenti le attività di verifica e/o i controlli per finalità di Sicurezza Integrata e/o Urbana, Prevenzione Ordine e/o Sicurezza Pubblica, Polizia Giudiziaria e/o Amministrativa, Prevenzione e Sicurezza Stradale
In ossequio al principio della *privacy by Design e by Default*, l'Amministrazione comunale e il Comando di Polizia Municipale hanno disciplinato l'uso di questi sistemi individuando le relative misure di sicurezza da osservare.
Non ne è previsto il loro utilizzo per attività di sanzionamento ai sensi del C.d.S. in modalità automatica, resta salva la possibilità di utilizzo dei fotogrammi e/o video quali prove documentali ai sensi della normativa vigente. Sono stati adottati i seguenti atti e adempimenti:

nomine degli autorizzati al trattamento dei Dati, secondo il *form* allegato alla presente come **"L - ATTO DI NOMINA VDS AD PERSONAM PL"**
adeguata formazione agli autorizzati al trattamento;
prevista **Informativa di I° Livello,** resa visibile e nota agli interessati attraverso l'accensione di spia luminosa di colore rosso posta sulla Body Cam nel momento di avvio della registrazione da parte dell'operatore di Polizia,
prevista e redatta apposita **informativa di II° livello** che è stata pubblicata sul sito istituzionale dell'ente comunale, allegato alla presente come **"F - INFORMATIVA ESTESA II LIVELLO VDS**"
redatto ad approvato apposito disciplinare di uso delle Body Cam, allegato alla presente come **"G - DISCIPLINARE TECNICO BODY CAM"**
sottoscrizione di apposito accordo sindacale, con le Organizzazioni Sindacali ai sensi dell'articolo 4 della Legge 300/1970 ("Statuto dei Lavoratori"), secondo il *form* allegato alla presente come **"D – ACCORDO SINDACALE VDS L. 300_70"** .

In riferimento a detti dispositivi di videoripresa mobile, l'Amministrazione ha appaltato solo la gestione tecnica ad una ditta esterna, lasciando **esclusa ogni attività di trattamento dei dati.**

3.5 Dispositivi di Geo localizzazione (GPS)

A seguito di episodi di aggressioni subite da operatori o pattuglie di Polizia Locale o di eventi nei quali vi era la necessità, da parte dei suddetti operatori, di avere un urgente ed immediato soccorso da parte di altri operatori, si è palesata anche la necessità organizzativa, da parte datoriale, di individuare ed avere a disposizione un idoneo mezzo tecnologico che permettesse la possibilità di individuare la posizione dell'operatore che richiedeva ausilio (geo localizzazione). Si tratta di dispositivo di localizzazione non di tipo *stand alone* ma integrato negli apparati radio. La posizione che viene trasmessa in caso di emergenza è quella della radio. A seguito di tali esigenze, nell'ottica di un percorso di *privacy by design e by default*, in adempimento a quanto previsto dalla normativa vigente, il Comune di Pisa Titolare del trattamento ha ritenuto di autorizzare l'utilizzo del Gps, da attivare solo ed esclusivamente a tutela della sicurezza del personale, in presenza di ragioni emergenziali che giustifichino la localizzazione del collega su strada, che è stato accompagnato dall'adozione dei seguenti atti e/o misure di sicurezza:

stipula con le rappresentanze sindacali, ai sensi dell'articolo 4 legge 300/70, di apposito accordo, siglato in data 21 febbraio 2018, allegato alla presente come **"M – ACCORDO ATTIVAZIONE GPS COMUNE OOSS (PROT 25099)";**
nomina degli autorizzati al trattamento dei Dati, allegato alla presente come **"C – ATTO DI NOMINA AUTORIZZATI VDS OPERATORI PL"**;
informativa specifica e dettagliata sul trattamento dei dati personali da fornire agli operatori di PL interessati;

formazione sull'utilizzo del sistema di geo localizzazione e modalità di trattamento al personale, che opera in Sala Operativa, anche assunto successivamente alla data di adozione di tali atti

conservazione dei file log di accesso al sistema GPS per almeno 36 mesi

- Con cancellazione sicura ed automatica di tali dati al termine sopra indicato

limitazione delle registrazioni audio radiofoniche a 30 giorni naturali e consecutivi

- Con cancellazione sicura ed automatica di tali dati al termine sopra indicato

4. Il Modello adottato per la redazione della presente DPIA

La normativa vigente non impone un modello predeterminato per la redazione della DPIA.
L'Autorità Garante italiana ha promosso l'utilizzo di un software per la valutazione di impatto, ideato a cura della autorità di controllo francese (CNIL) che però non risulta adeguato di fronte a normative speciali o complesse come quella italiana in materia di videosorveglianza. In ragione di quanto sopra, per la presente DPIA, è stata adottata la metodologia proposta da ENISA (*European Union Agency for Cybersecurity*).
Come già illustrato, scopo della presente DPIA è quello di valutare i rischi connessi ai trattamenti dei dati derivanti dall'utilizzo dei sistemi di videosorveglianza sopra descritti, e verificare se occorra attuare un'implementazione delle esistenti misure di sicurezza, al fine di mitigare il rischio di violazione di dati personali, fino a portarlo ad un livello accettabile.
Ai sensi dell'art. 35, comma 7, GDPR, e dell'art. 23 D.Lgs 51/2018, la DPIA deve contenere almeno:

1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. una valutazione dei rischi per i diritti e le libertà degli interessati;
4. le azioni 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 regolamento e alla direttiva, tenuto conto dei diritti degli interessati e degli altri soggetti coinvolti.

La **procedura di valutazione del rischio** si basa su **quattro macro-fasi** secondo la seguente sequenza:

- **Fase 1**: Definizione dell'operazione di trattamento e del suo contesto
- **Fase 2**: Comprensione e valutazione dell'impatto
- **Fase 3**: Individuazione delle possibili minacce e valutazione della probabilità di accadimento
- **Fase 4**: Valutazione del rischio (combinando l'impatto con la probabilità di accadimento)

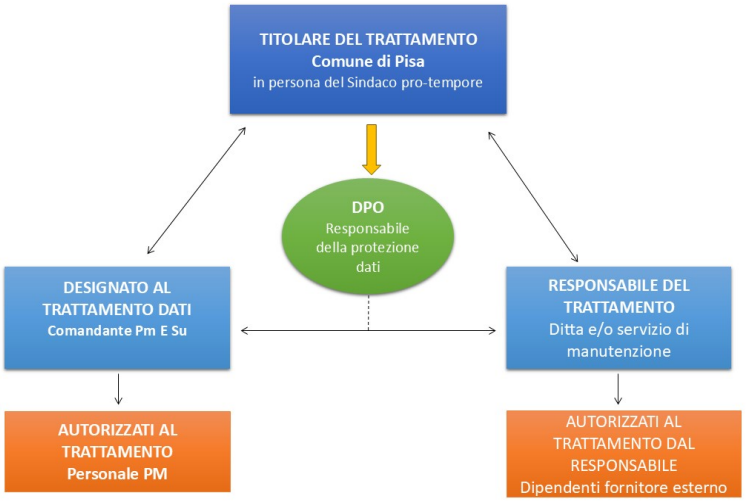
Attraverso la valutazione del rischio, si possono individuare ed adottare le misure di sicurezza tecniche e organizzative che risultano necessarie.

5. Definizione dell'operazione di trattamento e del suo contesto (Fase 1)

5.1 Organigramma, ruoli, responsabilità

L'Organigramma Privacy

L'Ente, nell'ambito del proprio sistema di gestione della *Privacy*, ha adottato un proprio organigramma che, per i trattamenti derivanti dai sistemi di VDS per finalità di ordine e sicurezza pubblica, può essere così rappresentato:



Titolare, Designati, Autorizzati al trattamento

Il **Titolare del trattamento** è il Comune in persona del Sindaco pro-tempore.
Secondo quanto previsto nell'organigramma *privacy* adottato con la Deliberazione di Giunta Comunale n. 47 del 4 aprile 2019, allegata alla presente sotto la lettera "**O – DELIBERA GC 47 DEL 4/4/2019 INDIVIDUAZIONE DESIGNATI E AUTORIZZATI AL TRATTAMENTO**, **Designato al trattamento dei dati** raccolti mediante telecamere collegate alla centrale operativa, lettura targhe, body cam, fototrappole e droni in uso alla Polizia Locale, è il Comandante della PM e SU.
Per i droni in uso all'Edilizia, Designato al trattamento è il Dirigente della Direzione Edilizia mentre, per i sistemi di videosorveglianza a circuito chiuso, non collegati alla centrale operativa, installati per finalità di tutela del patrimonio, mobiliare o immobiliare, o per sicurezza degli accessi ai luoghi di lavoro, Designato al trattamento dei dati sarà il Dirigente della direzione che ne ha richiesto l'installazione.
Il Designato è chiamato a mettere in atto le misure tecniche e organizzative necessarie a garantire un livello di sicurezza adeguato, nonché a rispettare pienamente quanto previsto dalla normativa in materia di protezione dati personali, nonchè le disposizioni del Regolamento di videosorveglianza.
Per esigenze organizzative, lo svolgimento di alcune operazioni del trattamento può essere affidato dal Titolare a soggetti terzi che, se trattano dati *per conto* del Comune di Pisa, sono nominati **Responsabili del trattamento** ex art. 28 GDPR attraverso un atto di nomina che contiene precise istruzioni per garantire adeguata protezione ai dati personali coinvolti.

Autorizzati al trattamento

Solo agenti e/o ufficiali di Polizia Locale con qualifica di agente e/o ufficiale di Polizia Giudiziaria e ausiliari di Pubblica Sicurezza possono accedere e trattare i dati personali raccolti mediante i sistemi di videosorveglianza comunale **collegati con la centrale operativa. Essi** sono **nominativamente autorizzati** e istruiti dal Comandante della PM, Designato al trattamento ed hanno ricevuto **idonea formazione** in tema di privacy, videosorveglianza, utilizzo dei sistemi, seguendo apposito programma formativo costituito da più moduli formativi, inerenti sia la "Normativa sulla Privacy" sia "Corso specifico per autorizzati all'utilizzo del sistema di videosorveglianza" in cui sono stati trattati i seguenti argomenti:

- **Parte Privacy**
- Programma del Corso Base: GDPR – Direttiva Polizia

- **Parte IVMS e DVR DMR**
- Programma del Corso Base gestione dati DMR e IVMS (VDS, LPR, "Dash Cam", Body Cam, Droni)

- **Procedure Operative e Misure di Sicurezza adottate per il trattamento in oggetto**

Ciascun autorizzato è dotato di proprie personali credenziali sicure di accesso ai sistemi per i quali è stato abilitato.
Personale amministrativo è autorizzato, mediante specifico atto di nomina contenente specifiche istruzioni per la protezione dei dati personali, al trattamento degli eventuali dati personali che possa derivare dall'utilizzo del sistema di videoripresa aeromobile in dotazione della Direzione Edilizia.

Per gli impianti di videosorveglianza a circuito chiuso, non collegati con la centrale operativa della PM, installati per finalità di tutela del patrimonio, mobiliare o immobiliare, o per sicurezza degli accessi ai luoghi di lavoro, personale amministrativo potrà essere autorizzato, mediante l'adozione di atti di nomina contenente specifiche istruzioni per la protezione dei dati personali, alla sola visione in tempo reale delle immagini a video ove necessari.

5.2 Descrizione dei trattamenti oggetto di valutazione

5.2.1 Sistema di videosorveglianza per finalità di sicurezza urbana e stradale

OMISSIS

Il trattamento dei dati raccolti mediante l'utilizzo dei sistemi di videosorveglianza del Comune di Pisa si configura come un **trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (art. 6, par 1, lett e) del GDPR**. La base giuridica è rappresentata dai sopra ricordati Decreto Ministro dell'Interno 5 Agosto 2008 (che all'art. 2 indica le molte finalità del trattamento già richiamate nel precedente paragrafo 3), dal D.Lg 23/02/2009, n.11 convertito nella Lg. 23/4/2009, n. 38, dal D. Lg. 20/02/2017, n.14, convertito nella Lg. 18/04/2017, n.48 c.d. "Pacchetto sicurezza Minniti" e altre normative speciali.

5.2.2 Descrizione degli strumenti di cui si compone il Sistema di Videosorveglianza realizzato – Parte Tecnica

Impianto di Video Sorveglianza Urbana integrata (ALLEGATI P; PP; PPP; PPPP).

OMISSIS

OMISSIS

OMISSIS

Altri sistemi di videosorveglianza

Con riguardo ai sistemi di videosorveglianza a tutela del patrimonio pubblico e della sicurezza nei luoghi di lavoro, ai dispositivi mobili a contrasto dell'abbandono dei rifiuti, ai sistemi di videoripresa indossabili, ai dispositivi di videoripresa aeromobili ed ai sistemi di geolocalizzazione si rinvia al Capitolo 4 e, più puntualmente, a quanto illustrato, per ciascuno di essi, nei rispettivi paragrafi (4.1 videosorveglianza a tutela del patrimonio pubblico e della sicurezza nei luoghi di lavoro; 4.4 dispositivi mobili a contrasto dell'abbandono dei rifiuti; 4.5 dispositivi di videoripresa aeromobili; 4.6 sistemi di videoripresa indossabili, Body Cam; 4.8 sistemi di geolocalizzazione) ciascuno dei quali dettaglia le misure di sicurezza organizzative adottate dall'Ente e richiama, in allegato, la pertinente documentazione sia amministrativa che tecnica, che forma parte integrante della presente DPIA.

5.2.3 Tipologia e caratteristiche del Trattamento Dati effettuato

Il trattamento dei dati, attuato attraverso l'utilizzo dei sistemi di videosorveglianza e/o lettura targhe, sopra esaminati presenta le seguenti caratteristiche:

Ambito di applicazione del trattamento

Modalità: Trattamento automatizzato di dati personali;
Area di Interesse: Territorio di competenza dell'ente;
Contesto: Aree, strade, luoghi pubblici o aperti al pubblico.
Mezzi: Sistemi di videosorveglianza costituiti da telecamere fisse e/o brandeggiabili e/o LPR e atte a consentire il monitoraggio e la visione di immagini in diretta e registrate, visibili da client della sala controllo della Polizia Municipale, Metadati di lettura targhe dei veicoli visibili da client della sala controllo della Polizia Municipale

Finalità del trattamento

- Monitorare la viabilità urbana per eventuali interventi in caso di necessità ai fini della sicurezza;
- Monitorare aree di pubblico interesse per la sicurezza;
- Costituire un deterrente per azioni vandaliche contro il patrimonio pubblico e privato;
- Ridurre e prevenire gli atti criminosi nelle aree sotto il controllo delle telecamere;
- Fornire un contributo documentale nell'eventualità di atti criminosi;
- Facilitare le operazioni ed i servizi di vigilanza delle forze dell'ordine;
- Ottimizzare e coordinare interventi in funzione di una gestione razionale delle risorse;
- Incrementare nella cittadinanza la percezione di prossimità delle Istituzioni;
- Tutela della sicurezza urbana;
- Tutela dell'ordine e della sicurezza pubblica;
- Prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali;
- Tutela della sicurezza stradale;
- Tutela ambientale;
- Tutela del patrimonio pubblico;
- Coadiuvare le attività, i compiti e obblighi istituzionali di Polizia;
- Fornire un ausilio alle attività istituzionali di protezione civile da parte della Polizia Locale e Ente;

Destinatari del trattamento

Ente Locale (solo per le finalità e attività istituzionali di Polizia previste da Specifiche normative).

Forze di Polizia (solo per finalità e attività inerenti compiti istituzionali di Polizia)
Autorità Giudiziaria (solo a seguito di esplicita richiesta per attività di indagine giudiziaria);
Ditta manutentrice nominata responsabile esterno
Non è previsto alcun trasferimento a Paesi extra UE)

Periodo di conservazione:

Come previsto dalla normativa di settore, sia di livello nazionale che di livello europeo (GDPR, Direttiva 680/16, D.Lgs 196/2003, D.Lgs 51 del 2018, Provvedimenti Garante Privacy, eventuale normativa o provvedimenti o circolari per casistiche specifiche) che dal Regolamento di videosorveglianza, i termini di conservazione devono essere previsti sulla base dei principi di necessità, pertinenza e non eccedenza, in ragione delle diverse tipologie di dati personali trattati e tenendo conto di ciascuna finalità in concreto perseguita.
In particolare, i dati relativi alla videosorveglianza per la tutela della sicurezza urbana, per l'ordine e la sicurezza pubblici, per la prevenzione e/o repressione dei reati, nonché per la tutela del patrimonio e/o per la sicurezza dei lavoratori, richiedono di essere conservati per un congruo periodo, tenendo di conto di eventuali periodi di festività e delle tempistiche inerenti la fase delle indagini e/o l'esposizione di eventuali denunce/querele agli organi di polizia. Il trattamento dei dati personali effettuato al di fuori dei motivi di ordine e sicurezza pubblica o urbana mediante l'uso di sistemi di videosorveglianza (non ad uso privato) non forma oggetto di legislazione specifica, salvi i principi generali dettati dal GDPR e dalle disposizioni generali in tema di protezione dei dati personali ancora in vigore. Il Garante della privacy, nei suoi provvedimenti sulla videosorveglianza del 29 aprile 2004 e dell'8 aprile 2010, si è espresso sulle tempistiche in situazioni e contesti specifici nei quali si utilizzi la videosorveglianza, affermando che, fatte salve le esigenze di ordine e sicurezza pubblici nonché prevenzione e repressione dei reati, per i quali trova applicazione la Direttiva UE 680/16 e D.Lgs 51/2018 (articolo 2, comma 2, lettera d del GDPR):

- nei casi in cui sia stato scelto un sistema che prevede la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita;
- nei casi non inerenti la sicurezza urbana o integrata, ordine e sicurezza pubblica o per attività di Polizia Giudiziaria, la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;
- solo in alcuni casi, per peculiari esigenze tecniche o per la particolare rischiosità dell'attività svolta dal Titolare del trattamento, può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti si ritiene non debba comunque superare la settimana (ad esempio, per alcuni luoghi, come le banche, può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina).

Il sistema impiegato è **programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni, da ogni supporto, allo scadere del termine previsto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati**.
Per quanto sopra, **in via precauzionale e cautelativa**, alla luce delle finalità previste per il sistema di videosorveglianza e lettura targhe oggetto di analisi e visto l'articolo 6 del regolamento sulla videosorveglianza adottato dall'ente, per quanto attiene ai tempi di conservazione dei dati, il Titolare ha ritenuto che i vari sistemi debbano essere conseguentemente programmati per poter tenere in memoria i relativi filmati o fotogrammi, dati delle targhe e dati della georeferenziazione come segue:

Telecamere con specifiche finalità di sicurezza urbana e sicurezza pubblica: **periodo di norma non superiore ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze investigative di**

polizia giudiziaria, con particolare riferimento ai varchi lettura targhe e ad altre esigenze correlate all'attività di istituto, comunque per il tempo strettamente necessario alla conclusione del relativo procedimento.
Telecamere Mobili con specifiche finalità di sicurezza urbana e sicurezza pubblica: **periodo di norma non superiore ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze investigative di polizia giudiziaria**, con particolare riferimento ai varchi lettura targhe e ad altre esigenze correlate all'attività di istituto, comunque per il tempo strettamente necessario alla conclusione del relativo procedimento.
Telecamere con finalità di tutela del patrimonio, non collegate con la centrale operativa ma a circuito chiuso: periodo di norma non superiore a 72 ore successive alla rilevazione, **fatte salve speciali esigenze investigative di polizia giudiziaria;**
Fototrappole con finalità di contrasto all'abbandono di rifiuti e prevenzione illeciti ambientali **periodo di norma di 7 giorni**, fatte salve diverse esigenze di Polizia. Eventuali necessarie e improcrastinabili esigenze tecniche connesse alla **gestione e manutenzione degli apparati** potrebbero comportare la necessità di sforare rispetto alla suddetta tempistica di **ulteriori 7 giorni naturali e consecutivi rispetto ai tempi previsti**.

5.2.4 Informativa agli Interessati ed esercizio dei diritti

Essendo i trattamenti necessari per l'esercizio di pubblici poteri dei quali è investito l'Ente in qualità di Titolare del trattamento, **il consenso degli interessati non è necessario** (art. 6, paragrafo 1, lettera e del GDPR 679/16 e art. 10 D. Lgs.vo 51/18).
L'informazione agli interessati è assicurata attraverso differenti strumenti:

1. Tutte le **aree soggette a videosorveglianza sono segnalate** attraverso il posizionamento **di appositi cartelli,** collocati nelle loro vicinanze, e contenenti la c.d. **informativa di primo livello** (allegati **E, EE, EEE**);
2. Sono state attuate nel tempo comunicazioni su idonei mezzi di diffusione (es: mass media locali);
3. Sul sito istituzionale dell'ente è stata istituita apposita pagina web, rubricata **Protezione Dati** dove trovasi pubblicata l'informativa completa per gli interessati, c.d. **informativa di secondo livello,** integrale, (allegato **F**), oltre alla modulistica necessaria ai fini dell'esercizio dei diritti dei cittadini, con indicazione dei relativi contatti.
4. Nella pagina dedicata ai regolamenti del sito web istituzionale dell'ente è pubblicato e liberamente consultabile il Regolamento comunale per l'utilizzo del sistema di videosorveglianza.

Attraverso l'informativa sono resi indicate le modalità per l'esercizio dei diritti da parte degli interessati. Il Comune con Circolare del Segretario generale prot. n.55026 del 23/5/2019, aggiornata con Circolare del Segretario Generale n. 65290 del 14/7/2020, ha adottato anche una specifica **procedura per l'esercizio dei diritti degli interessati** e, nella sezione **Protezione Dati** del sito istituzionale, tiene pubblicato il modulo per l'esercizio dei diritti.
Il sistema sopra descritto dimostra di presentare garanzie adeguate in termini di conoscenza specialistica, affidabilità, risorse ed attuazione di misure tecniche e organizzative.

6. Comprensione e valutazione dell'impatto (Fase 2)

Per calcolare il rischio è necessario, in via preliminare, classificare i fattori che lo determinano quindi l'**impatto** (**I**) che può derivare sugli interessati da una "alterazione" del dato personale e la **probabilità** (**P**) del suo verificarsi.

6.1 La Scala dei possibili Livelli di Impatto

Sulla base dell'analisi e risultanze della fase precedente (Fase 1), si procede a valutare l'impatto, sui diritti e sulle libertà fondamentali delle persone fisiche, che una perdita di sicurezza dei dati potrebbe cagionare.
Per tale analisi, si considereranno quattro livelli di impatto (Basso, Medio, Alto, Molto Alto) e relativi possibili effetti come di seguito illustrato:
Livello Basso: valore **1. Possibili conseguenze**: l'impatto per gli interessati produce scarsi disagi, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);

Livello Medio: valore **2. Possibili conseguenze**: l'impatto per gli interessati produce significativi disagi, superabili con alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.);

Livello Alto: valore 3. **Possibili conseguenze**: l'impatto per gli interessati produce significative conseguenze che dovrebbero essere in grado di superare, anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.);

Livello Molto Alto: valore 4. **Possibili conseguenze**: l'impatto per gli interessati produce conseguenze irreversibili, che non saranno in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

6.2 Determinazione dei Livelli di Impatto

Per quanto riguarda le tipologie di impatto da considerare, è buona prassi concentrare l'attenzione sul paradigma R.I.D. della ISO 27001, per la quale un dato personale può dirsi **sicuro** quando è
Riservato (l'accesso alle informazioni è limitato a un gruppo preventivamente definito ed autorizzato ad avere questo accesso),
Integro (l'integrità è caratterizzata da due aspetti che sono: correttezza e completezza delle informazioni),
Disponibile (è il grado in cui le informazioni sono disponibili all'utente e al sistema informativo nel momento in cui queste vengono richieste).
Il **Livello di Impatto** sui diritti e le libertà dei soggetti interessati di un attività di trattamento, in caso di compromissione della sicurezza (ovvero di riservatezza, integrità e la disponibilità) di un dato personale, varia a seconda del tipo di dato trattato, del contesto specifico, dell'organizzazione interna, come rappresentato nella seguente tabella:

Tabella Metrica dei Livelli di impatto						Legenda: N.A. = Non Applicabile
Criterio	Descrizione		Livello Impatto Corrispondente			
	Insieme principale	Sotto-insieme specifico	Basso	Medio	Alto	Molto Alto
	Dati economico-finanziari non amministrativi		-	-	-	X
	Monitoraggio sistematico su larga scala e/o di geolocalizzazione		-	-	-	X
	Dati di videosorveglianza ad elevata risoluzione		-	-	-	X
	Trattamenti di dati su larga scala		-	-	-	X
		Origine razziale o etnica	-	-	-	X
		Appartenenza a partiti	-	-	-	X

Categorie di dati personali		*Appartenenza a sindacati*	-	-	-	X
		Appartenenza ad associazioni a carattere religioso	-	-	-	X
		Appartenenza ad associazioni a carattere filosofico	-	-	-	X
		Appartenenza ad associazioni a carattere politico	-	-	-	X
		Appartenenza ad associazioni a carattere sindacale	-	-	-	X
	Dati relativi alla salute		-	-	-	X
	Dati genetici		-	-	-	X
	Dati biometrici		-	-	-	X
	Dati di utilizzo di servizi e strumenti		-	-		X
	Dati multimediali		-	-	X	-
	Dati di videosorveglianza a bassa risoluzione		-	-	X	-
	Dati di Log di sistema		-	-	X	-
	Dati anagrafici		-	X	-	-
	Dati economico- finanziari		-	X	-	-
	Dati anonimizzati		X	-		-
Categorie di soggetti interessati	*Minori o altri soggetti svantaggiati*		-	-	-	X
	Cittadini		-	-	X	-
	Dipendenti		-	-	X	-
	Fornitori		-	X	-	-
Finalità del trattamento	*Profilazione*		-	-	-	X
	Geo-localizzazione		-	-	-	X
	Controllo o tracciamento della persona o veicoli		-	-	-	X
	Big Data per profilazione		-	-	-	X
	Servizi accessori		-	-	X	-
	Videosorveglianza		-	-	X	-
	Big data per fini statistici		-	X	-	-
	obbligo contrattuale, precontrattuale, adempimento legale, legittimo interesse)		X	-	-	-
	Compiti Istituzionali/obbligatori		X	-	-	-
Trasferimento dati verso Paesi extra UE	*Trasferimento previsto*		N.A.	N.A.	N.A.	N.A.
	Trasferimento NON previsto		X	-	-	-
Tipologia di soluzioni tecnologiche o organizzative	*Utilizzo innovativo o adozione di soluzioni tecnologiche*		N.A.	N.A.	N.A.	X
	Utilizzo di tecnologie tradizionali		X	-	-	-

Conseguenza del trattamento	*Inibizione all'esercizio anche di un solo diritto o all'utilizzo di un solo servizio da parte dell'interessato*		-	-	-	-
	Nessuna inibizione all'esercizio anche di un solo diritto o all'utilizzo di un solo servizio da parte dell'interessato		X	-	-	-

6.3 Risultanze dei Livelli di Impatto

Sulla base dell'analisi condotta, risulta che il trattamento di dati personali in esame è strutturato nel modo seguente:

Descrizione dell'operazione di elaborazione: Videosorveglianza Sicurezza Integrata
Categorie di dati: Video e Metadati - Personali comuni;
Finalità del trattamento: Sicurezza Urbana, prevenzione ordine e sicurezza pubblica, prevenzione e repressione dei reati, tutela della incolumità e sicurezza dei lavoratori, tutela del patrimonio pubblico;
Categorie di soggetti interessati: Abitanti, Residenti, Cittadini, Lavoratori, Utenti della Strada;
Numerosità dei dati trattati: effettuata l'elaborazione dei dati su larga scala per motivi di interesse pubblico;
Tipologie di soluzioni tecnologiche o organizzative: utilizzo di tecnologie di Videosorveglianza e trattamento di metadati su larga scala;
Destinatari dei Dati Personali

a) **Esterni:** Invio ad Autorità Giudiziaria e/ altre Forze di Polizia in caso di reati
b) **Interni:** Uffici di Polizia Amministrativa o Giudiziaria

Sistema di processione dei dati utilizzato: Il trattamento è effettuato presso la sede del Titolare del trattamento
Trasferimento dati verso paesi extra-UE: non è previsto il trasferimento dei dati extra UE.

Alla luce dei livelli di impatto riportati nella tabella e applicabili al caso specifico, si può affermare che, **secondo una valutazione prudenziale, in assenza di misure di sicurezza, il livello di impatto complessivo del trattamento** per i diritti e le libertà degli interessati **potrebbe ritenersi ALTO.**

7. Definizione e individuazione di possibili minacce e valutazione della loro probabilità di accadimento (Fase 3)

Una minaccia è qualsiasi circostanza o evento che può potenzialmente incidere negativamente sulla sicurezza dei dati personali. In questa fase, l'obiettivo del Titolare del trattamento è comprendere le minacce legate all'ambiente generale del trattamento dei dati personali (esterno o interno) e valutarne la probabilità (probabilità di accadimento della minaccia). A tale riguardo sono presi in considerazione diversi livelli e tipi di minacce con riguardo alla riservatezza, all'integrità e alla disponibilità dei dati personali.
Analogamente al caso della valutazione dell'impatto, la valutazione della probabilità di accadimento della minaccia è stimata tenendo di conto del contesto, dei mezzi e delle finalità di trattamento.
I livelli di probabilità di accadimento della minaccia, sono tre:

Livello della Minaccia	Probabilità Accadimento
Basso	Improbabile che la minaccia si concretizzi.
Medio	Possibile che la minaccia si materializzi.
Alto	Probabile che la minaccia si concretizzi.

Le verifiche dovranno essere incentrate su **quattro principali aree di valutazione**, relative a **elaborazione e trattamento dei dati**, e nello specifico:

Rete e risorse tecniche (hardware e software)
Processi/Procedure relative al Trattamento dei Dati Personali
Soggetti e mezzi coinvolti nell'operazione di trattamento
Settore di attività e scala del trattamento

Il ***Cyber Risk*** in particolare è poi da distinguere in due macro-fattispecie di rischio:

Rischio IT puro:
- rischi derivanti da eventi accidentali sui sistemi IT, come l'errore umano, utilizzo errato di software, etc.

Rischio *Cyber Crime*:
- rischi connessi ad attività criminali dolose, mediante l'uso della rete.

L'ICT *Security Assessment* è una metodologia che permette di misurare il proprio livello di rischio informatico, di valutare l'efficacia delle misure di sicurezza adottate e/o la necessità di implementarne di ulteriori.
Il Titolare può ridurre il livello di *cyber-risk* e la possibilità del suo verificarsi tramite verifiche periodiche, attraverso adeguati strumenti e metodologie, che forniscano anche indicazioni sulle eventuali ulteriori misure da attuare. Chiaramente, ogni volta che da tali verifiche dovesse emergere un aumento del rischio e/o la necessità di implementazione di misure, la DPIA dovrà essere adeguatamente revisionata.
Al termine dell'analisi, **la probabilità di accadimento della minaccia è ottenuta come il più alto dei punteggi ottenuti per ciascuna delle aree sopra individuate.**

8. Valutazione del rischio: combinazione della probabilità e dell'impatto (Fase 4)

8.1 Metodologia analitica adottata per la stima "quantitativa" del rischio

Secondo la UNI EN ISO 12100-1, la **stima del rischio** si effettua correlando la gravità del danno con la probabilità del suo accadimento (**I x P= RISCHIO**).
Ai fini della stima, si indica con **"I" l'impatto ovvero la gravità del danno**, mentre con "**P" la probabilità del verificarsi dell'evento**.
La corrispondenza tra il valore del livello di impatto e il relativo livello di probabilità di accadimento dà come risultato il Livello di Rischio (**R)** a seconda del quale conseguiranno raccomandazioni di azioni correttive da realizzare.
La "**Matrice di Corrispondenza**" adottata per il "Calcolo del Rischio" è la seguente:

Tabella Risultanze Analisi Rischi					
		Livello di Impatto Complessivo			
		Basso	Medio	Alto	Molto Alto
Probabilità Accadimento Minacce Globali	Basso				
	Medio				
	Alto				
Legenda Livelli Probabilità:	Basso (1)	Medio (2)		Alto (3)	
Legenda Livelli Impatto:	Basso (1)	Medio (2)		Alto (3)	Molto Alto (4)

8.2 Individuazione delle misure di sicurezza necessarie e calcolo del livello di rischio

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 del GDPR è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per lo stesso motivo, dopo il 25 maggio 2018, data di entrata in vigore nell'ordinamento italiano del GDPR, non è più sufficiente l'adozione delle c.d "misure minime" di sicurezza (previste dall'art. 33, ormai abrogato, del Codice in materia di protezione dei dati personali) poiché la valutazione dell'adeguatezza delle misure è rimessa, caso per caso, al Titolare e al Responsabile esterno del trattamento in rapporto ai rischi specificamente individuati.

Per la riduzione del livello di rischio del trattamento, per ciascuna delle minacce possibili, tenuto conto del modello organizzativo, sono state individuate adeguate misure di sicurezza, riportate nella seguente tabella denominata "**Tabella delle Misure di Sicurezza",** già implementate o in fase di implementazione, necessarie a garantire una mitigazione del rischio fino a portarlo a livelli accettabili.

Contesto Misura di Sicurezza	DESCRIZIONE DELLA MISURA DI SICUREZZA
Aspetti di sicurezza nella gestione della Continuità Operativa	OMISSIS
Consapevolezza della sicurezza delle informazioni, educazione e formazione	OMISSIS
Controllo degli accessi	OMISSIS

Politica di controllo degli accessi	OMISSIS
Copia di sicurezza o Sicurezza dei Dati (Back-Up)	OMISSIS
Dispositivi mobile	OMISSIS
Gestione degli incidenti di sicurezza (Data Breach)	OMISSIS
Gestione della vulnerabilità tecnica e Sicurezza nei processi di sviluppo e supporto	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
Gestione delle risorse IT	OMISSIS
	OMISSIS
Politica di sicurezza	OMISSIS
Procedure operative e responsabilità	OMISSIS
	OMISSIS
Rapporti con i fornitori	OMISSIS
	OMISSIS
Registrazione e monitoraggio	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
Requisiti di sicurezza dei sistemi	OMISSIS

	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
Sicurezza delle comunicazioni	OMISSIS
	OMISSIS
Sicurezza delle operazioni	OMISSIS
Sicurezza delle risorse umane	OMISSIS
Sicurezza delle risorse umane	OMISSIS
Sicurezza fisica e ambientale	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
	OMISSIS
Smaltimento dei supporti e S Smaltimento dei supporti e Smaltimento o riutilizzo sicuro dell'attrezzatura o riutilizzo sicuro dell'attrezzatura	OMISSIS

8.3 Calcolo del livello di rischio a seguito dell'adozione di misure di sicurezza individuate

Alla luce delle misure di sicurezza individuate e adottate, è stato **calcolato, per ciascuna minaccia e relativo impatto, il conseguente** "**Rischio Residuo Risultante**" secondo quanto riportato nelle seguente tabelle:

Analisi Impatto Globale Applicate Misure di Sicurezza Individuate				
Criterio	**Descrizione**	**Livello**	**Valore**	**Giustificazione**
Riservatezza	divulgazione non autorizzata (perdita di riservatezza) di dati personali.	Basso	1	Procedure e criteri di controllo prestabiliti e permanenti oltre che ad adeguata formazione, preventiva e periodica, e responsabilizzazione dei designati garantiscono adeguati livelli di riservatezza
Integrità	alterazioni non autorizzate (perdita di integrità) dei dati personali.	Basso	1	Il sistema memorizza in modo automatizzato i dati e li rende inalterabili anche agli amministratori di sistema
Disponibilità	Possibile distruzione o perdita (perdita di disponibilità) non autorizzata di dati personali	Basso	1	Uno o più sistemi di ridondanza dei database e/o servizi (server failoure, backup, sistemi RADI, ecc) e servizi di manutenzione tecnica adeguati garantiscono la disponibilità o ripristino dei dati in tempi brevi.
Risultanze Livello di impatto complessivo		Basso	1	

Di seguito si riportano i dati relativi alla **probabilità di accadimento delle possibili minacce** come mitigate dalle misure di sicurezza adottate o in corso di adozione:

Minacce rilevanti per il rischio privacy		Probabilità Accadimento	Valore
Rete e risorse tecniche (hardware e software)	*Trattamento dei dati personali effettuati tramite Internet*	Basso	1
	Accesso a un sistema interno di elaborazione dei dati personali tramite Internet	Basso	1
	Interconnessione con un altro sistema o servizio informatico esterno o interno (Rispetto alla organizzazione in oggetto)	Basso	1
	Possibilità per personale non autorizzato di accedere facilmente all'ambiente di elaborazione dei dati	Basso	1
	Accesso Illegittimo ai dati	Basso	1
	Attacchi informatici	Basso	1
	Furto di identità	Basso	1
	Intercettazione delle comunicazioni	Basso	1
	Furto o smarrimento di apparati hardware	Basso	1
	Perdita disponibilità per guasto HW	Basso	1
	Abuso di privilegi di accesso	Basso	1
	Perdita integrità per guasto HW	Basso	1
Probabilità Accadimento Minacce di Area	**Bassa**	**Valore Area Equivalente**	**1**
Processi e procedure relative al Trattamento dei Dati Personali	*Definizione dei ruoli e responsabilità in relazione al trattamento dei dati personali*	Basso	1
	Utilizzo della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione	Basso	1
	Connessione ed utilizzo di propri dispositivi per connettersi al sistema di elaborazione dei dati personali	Basso	1
	Trasferimento, archiviazione o elaborazione dati personali al di fuori dei locali dell'organizzazione	Basso	1
	Utilizzo dei file di LOG per le attività di trattamento dei dati personali	Basso	1
	Errori nei processi di elaborazione dei dati	Basso	1
	Interrogazioni improprie su basi dati	Basso	1
	Modifica non autorizzata dei dati	Basso	1

	Cancellazione volontaria o accidentale dei dati	**Basso**	**1**
	Utilizzo improprio di software o servizi	**Basso**	**1**
Probabilità Accadimento Minacce di Area	**Bassa**	**Valore Area Equivalente**	**1**
Soggetti e mezzi coinvolti nell'operazione di trattamento	*Quantificazione livelli e diritti di accesso ai dati da parte del personale designato al trattamento dei dati personali*	**Basso**	**1**
	Operazione di trattamento e memorizzazione dei dati eseguite presso contraenti e/o terzi soggetti	**Medio**	**2**
	Definizione degli obblighi delle parti o designati coinvolte nel trattamento dei dati personali	**Basso**	**1**
Probabilità Accadimento Minacce di Area	**Bassa**	**Valore Area Equivalente**	**2**
	Designati e loro formazione e informazione in merito alle questioni di sicurezza inerenti il trattamento	**Basso**	**1**
	Distruzione e/o archiviazione sicure dei dati necessari alle operazioni di trattamento	**Basso**	**1**
	Perdita del controllo dei dati	**Basso**	**1**
	Diffusione Illegittima di dati a terzi soggetti non autorizzati o competenti	**Basso**	**1**
Probabilità Accadimento Minacce di Area	**Bassa**	**Valore Area Equivalente**	**1**
Settore di operatività e scala del trattamento	*Livello esposizione ad attacchi informatici del settore specifico al trattamento*	**Basso**	**1**
	Attacchi informatici o altri tipi di violazione della sicurezza subiti negli ultimi due anni	**Basso**	**1**
	Segnalazioni e/o reclami effettuati o ricevuti negli ultimi due anni in merito alla sicurezza del sistema informatico utilizzato per il trattamento dei dati personali	**Basso**	**1**
	Il numero degli interessati e la quantità di dati personali oggetto del trattamento	**Medio**	**2**
	Monitoraggio sistematico, Videosorveglianza su larga scala	**Medio**	**2**
	Pratiche di sicurezza specifiche per il settore di attività del trattamento	**Basso**	**1**
	Danno reputazionale all'interessato	**Basso**	**1**
	Possibile Discriminazione	**Basso**	**1**
	Corrispondenze o combinazione di insiemi di dati	**Basso**	**1**
	Perdite finanziarie	**Basso**	**1**
	Danni fisici o psicologici	**Basso**	**1**
	Svantaggi economici e sociali	**Basso**	**1**
Probabilità Accadimento Minacce di Area	**Media**	**Valore Area Equivalente**	**2**

La probabilità di accadimento della minaccia è ottenuta come il più alto dei punteggi ottenuti per ciascuna delle aree sopra individuate. Ne consegue:

Probabilità Accadimento Minacce Globali	**Media**
Valore Globale Equivalente	**2**
Risultanze Livello di impatto complessivo	**Basso**
Valore	**1**

Tabella Risultanze Analisi Rischi in Origine

		Livello di Impatto Complessivo			
		Basso	Medio	Alto	Molto Alto
Probabilità Accadimento Minacce Globali	Basso				
	Medio	X			
	Alto				

Legenda Livelli Probabilità:	Basso (1)	Medio (2)	Alto (3)	
Legenda Livelli Impatto:	Basso (1)	Medio (2)	Alto (3)	Molto Alto (4)

9. Esito finale e conclusioni della DPIA

In considerazione delle finalità, della natura, del contesto, delle modalità e della tipologia di dati oggetto del trattamento, **viste le misure di sicurezza sopra individuate e adottate, alcune in fase di completamento,** i trattamenti di dati effettuati e descritti nel presente documento comportano **un livello di Rischio per i diritti e le libertà degli interessati da ritenersi**

BASSO

Sulla base delle valutazioni sopra enunciate e della documentazione allegata, il sottoscritto Comandante, in qualità di Designato al trattamento dei dati derivante dai sistemi di videosorveglianza e lettura targhe oggetto della presente DPIA, sentito il Responsabile della Protezione Dati dell'ente, che ha espresso parere positivo riportato in calce, dichiara l'esito della presente Valutazione di impatto sulla protezione dei dati

POSITIVO

in quanto, a seguito dell'individuazione e attuazione delle misure organizzative e di sicurezza sopra descritte allo stato attuale non sussiste un rischio elevato per i diritti e le libertà delle persone e i dati personali relativi all'insieme dei trattamenti in esame sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e aggiornati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti;
- trattati in maniera da garantire un'adeguata sicurezza e protezione dei dati personali, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)..

Pisa, martedì 9 dicembre 2025.

Per il Comune Titolare del trattamento
Il Comandante della PM e SU
Designato al trattamento dei dati

Preso atto di quanto descritto nella presente DPIA e nella documentazione tecnica ad essa allegata in ordine alle misure di sicurezza tecniche (Allegati P, PP, S, T, U, V, W, Y, Z, Zbis) e dato atto dell'adozione delle misure di sicurezza organizzative si esprime parere positivo.

Il DPO dell'Ente
avv.to Veronica Malfatti

Allegati

Documentazione Amministrativa:

A. - Atto di nomina responsabile esterno;
AA. – Atto di nomina responsabile esterno con funzioni di Amministratore di sistema
B. - Atto di nomina amministratore di sistema interno;
C. - Atto di Nomina autorizzati VDS Operatori di PL
CC - Atto di Nomina autorizzato VDS Luoghi di lavoro;
D. - Accordo sindacale vds l. 300_70;
E. - Informativa I livello VDS;
EE. – Informativa I livello Luoghi di lavoro
EEE – Informativa I livello VDS Ambiente
F - Informativa estesa II livello VDS;
G - Disciplinare tecnico BODY CAM
H- Disciplinare tecnico VDS mobile
I – Atto di nomina VDS drone Edilizia
J - Atto utilizzo droni informativa e prescrizioni
JJ – Informativa I livello drone edilizia
JJJ – Informativa II Livello drone Edilizia
L - Atto di nomina vds mobile ad personam PL (dash cam, Body Cam, fototrappole, drone PM)
LL - Informativa I livello drone PL
LLL-Informativa II Livello drone PL
M – Accordo attivazione GPS Comune OOSS
N. – Accordo titolarità autonoma
O - Delibera GC n 47 del 04_04_2019 individuazione designati e autorizzati al trattamento
Q - Patto sicurezza Pisa 2018
R - Procedura gestione *data breach* rev dic 2022

Documentazione Tecnica:

P - OMISSIS
PP - OMISSIS
PPP - OMISSIS
PPPP - OMISSIS
S - OMISSIS
T - OMISSIS
U - OMISSIS
V - OMISSIS
W - OMISSIS
Y - OMISSIS
Z - OMISSIS
Z *bis* - OMISSIS