Comune di Santeramo in Colle

Città Metropolitana di Bari

DATA PROTECTION IMPACT ASSESSMENT

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

art. 35 reg. (UE) 2016/679 GDPR e art. 23 d. lgs. 51/2018

Data prima versione: 6/12/2024

Versione corrente: 1.1 del 7/8/2026

Scadenza del presente documento / data revisione: 3/2/2027

Valutazione realizzata dal Comune di Santeramo in Colle, in qualità di titolare del trattamento, con il supporto tecnico di Ethica Societas UPLI società cooperativa sociale onlus.

SOGGETTI COINVOLTI

Legale rappresentante del titolare del trattamento-DC: avv. Vincenzo Luciano Casone, sindaco;

Designato ai trattamenti esclusi dal GDPR: comm. sup. dott. Vincenzo Caporusso, ;

Responsabile della Protezione dei Dati/DPO: Giuseppe Nuzzolese, presso Municipio di Santeramo in Colle, piazza dottor Simone, 8 - Santeramo in Colle (BA), soggetto interno;

Coordinatore del team di valutazione:

Revisore della valutazione:

INDICE

PARTE A-Premessa

Sezione A1-Introduzione

Il presente documento è stato svolto ai sensi dell'art. 35 del Regolamento (UE) 2016/679 per i trattamenti generali e dell'art. 23 del decreto legislativo 51/2018 relativamente ai trattamenti finalizzati alla prevenzione, indagine, accertamento, perseguimento di reati, esecuzione di sanzioni penali, prevenzione e salvaguardia della sicurezza pubblica, seguendo le Linee guida WP29 del 4 ottobre 2017 *"in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del regolamento (UE) 2016/679*" e le Linee guida EDPB 3/2019 *"sul trattamento dei dati personali attraverso dispositivi video"*.

Per la valutazione e misurazione del rischio si sono utilizzate le regole definite dalle vigenti norme universali di armonizzazione e standardizzazione definite dall'ISO-International Organization for Standardization e, in particolare, dalla ISO 31000:2018 "*Gestione del rischio - Linee guida*", in vigore dal 17/05/2018, dalla UNI CEI EN IEC 31010:2019 "*Gestione del rischio - Tecniche di valutazione del rischio*", in vigore dal 19/12/2019, e dalla ISO/IEC 29134:2023 "*Information Technology - Security techniques - Guidelines for privacy impact assessment*", in vigore dall'8 maggio 2023.

L'attuale versione 1.1 definitiva, valida sino a tutto il 3/2/2027, costituisce aggiornamento e ampliamento del precedente documento che segue e sostituisce la versione realizzata in data 6/12/2024 con validità sino al 6/3/2025.

A1.1 Incarico per il supporto tecnico nella valutazione

La presente valutazione d'impatto sulla protezione dei dati-DPIA è stata svolta con il supporto tecnico di Ethica Societas UPLI società cooperativa sociale onlus, attraverso il proprio team di esperti e periti valutatori, giusto affidamento di incarico da parte del Comune di Santeramo in Colle, titolare del trattamento, come da determinazione del responsabile della Polizia Locale n. 1456/RG del 29/07/2026.

La responsabilità finale della valutazione, dell'accettazione del rischio residuo, dell'attuazione delle misure di mitigazione e dell'eventuale consultazione preventiva dell'Autorità di controllo resta in capo al titolare del trattamento.

A1.2 Cronologia delle versioni

VER.	DATA	CAUSALE	SCADENZA
1.0	6/12/2024	prima versione	6/3/2025
1.1	7/8/2026	aggiornamento e ampliamento del precedente documento	3/2/2027

A1.3 Obblighi di aggiornamento e scadenza

In via generale, l'aggiornamento del presente atto come di tutte le misure di protezione dei dati personali è alla base del rispetto del principio di accountability (art. 24 par. 1 GDPR[1]), è necessario quindi svolgere ed essere in grado di dimostrare che si esegua regolarmente la verifica della sicurezza del trattamento e l'eventuale adeguamento delle conseguenti misure di mitigazione del rischio in tutti i casi e per tutte le finalità, anche per i trattamenti esclusi dal GDPR (art. 15 d. lgs. 51/2018[2]).

In particolare, l'aggiornamento della valutazione d'impatto sulla protezione dei dati è richiesta dalle norme vigenti per verificare che il trattamento dei dati personali sia effettuato conformemente alle prescrizioni qui contenute e per controllare se insorgano variazioni del rischio (art. 35 par. 11 GDPR[3]).

Ciò vale anche per le finalità di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali e per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, che sono anch'essi valutati nel presente atto, per i quali le norme prescrivono il riesame e l'aggiornamento continuo delle misure di protezione dei dati da parte del titolare del trattamento.

Per gli obblighi sopra indicati e per le motivazioni argomentate di seguito, si indica la scadenza della presente valutazione d'impatto-DPIA **nel termine di 180 giorni e quindi entro il 3/2/2027**.

A1.4 Normativa di riferimento e indicazioni abbreviate

Per la redazione del presente atto si è fatto riferimento ai seguenti testi normativi, intendendosi anche nelle loro successive modificazioni e integrazioni, che per brevità saranno indicati come di seguito elencati in ordine alfabetico di abbreviazione:

ATSO: legge 13 maggio 1978 n. 180 *'Accertamenti e trattamenti sanitari obbligatori'*.

C.c.: regio decreto 16 marzo 1942, n. 262 "*Approvazione del testo del Codice civile*".

C.d.N.: regio decreto 30 marzo 1942, n. 327 "*Approvazione del testo definitivo del Codice della navigazione*".

C.d.S.: decreto legislativo 30 aprile 1992, n. 285 "*Nuovo codice della strada*".

CAD: decreto legislativo 7 marzo 2005, n. 82 "*Codice dell'amministrazione digitale*".

CCNL: Contratto collettivo nazionale di lavoro del comparto funzioni locali, attualmente vigente nella versione sottoscritta il 16 novembre 2022 per il triennio 2019-2021.

Codice della privacy: decreto legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", come modificato

[1] Reg. (UE) (UE) 2016/679 GDPR, art. 24 (Responsabilità del titolare del trattamento): «*[...] Dette misure sono riesaminate e aggiornate qualora necessario.*».

[2] D. lgs. 51/2018 art. 15 (Obblighi del titolare del trattamento): «*1. Il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del presente decreto. 2. Le misure di cui al comma 1 sono riesaminate e aggiornate qualora necessario e, ove proporzionato rispetto all'attività di trattamento, includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.*».

[3] Reg. (UE) (UE) 2016/679 GDPR, art. 35 (Responsabilità del titolare del trattamento): «*11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.*».

e integrato dal decreto legislativo 10 agosto 2018 n. 101.

Codice della protezione civile: il titolo del decreto legislativo 2 gennaio 2018 n. 1.

C.p.p.: decreto del Presidente della Repubblica 22 settembre 1988, n. 447 "*Approvazione del codice di procedura penale*".

D. lgs. 152/2006: decreto legislativo 3 aprile 2006, n. 152 "*Norme in materia ambientale*" aggiornato con le modifiche introdotte dalla legge 9 ottobre 2023, n. 137 "*Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione*" che, a decorrere dal 10 ottobre 2023, ha esteso la sanzione penale anche agli abbandoni di rifiuti da parte dei privati (art. 255).

D. lgs. 151/2015: decreto legislativo 14 settembre 2015, n. 151 "*Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183*" (Jobs Act) che ha riscritto l'art. 4 dello Statuto dei Lavoratori di cui alla legge 20 maggio 1970 n. 300, nella parte relativa all'utilizzo dei sistemi di videosorveglianza) e l'art. 171 del d. lgs. 30 giugno 2003 n. 196, nella parte relativa all'utilizzabilità ai fini del diritto del lavoro delle informazioni acquisite con sistemi audiovisivi.

D. lgs. 51/2018: decreto legislativo 18 maggio 2018, n. 51 "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*".

Direttiva polizia: direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio d'Europa, del 27 aprile 2016, relativa alla *protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio* (c.d. direttiva di polizia), trattandosi di una direttiva occorre il recepimento statale che, per l'Italia, è avvenuto con il decreto legislativo 18 maggio 2018, n. 51.

Documento d'indirizzo DPO: GPDP "*Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*" allegato al provvedimento del 29 aprile 2021 n. 186.

D.P.R. 15/2018: decreto del Presidente della Repubblica 15 gennaio 2018, n. 15 "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*".

GDPR: regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio d'Europa, del 27 aprile 2016 "*Regolamento generale sulla protezione dei dati"*[4], titolo originale "*General Data Protection Regulation*"[5] da cui l'acronimo GDPR.

L. 353/2000: legge 21 novembre 2000 n. 353 '*Legge-quadro in materia di incendi boschivi*'.

L. 689/1981: legge 24 novembre 1981 n. 689 '*Modifiche al sistema penale*'.

L. 65/1986: legge 7 marzo 1986 n. 65 '*Legge-quadro sull'ordinamento della polizia municipale*'.

L. 48/2017: legge 18 aprile 2017 n. 48 '*Conversione in legge con modificazioni del decreto-legge 20 febbraio 2017, n. 14, recante disposizioni urgenti in materia di sicurezza delle città'* (c.d. decreto Minniti), che ha potenziato l'interscambio dei dati tra le forze di polizia locali e nazionali e ha rafforzato la cooperazione tra gli enti locali e lo Stato anche nei trattamenti di dati mediante strumenti di videosorveglianza.

L. 205/2021: legge 3 dicembre 2021 n. 205 '*Conversione in legge con modificazioni del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali'* (c.d. decreto capienze), che ha riformato il trattamento dei dati personali per finalità di polizia e sicurezza dello Stato, anche nel trattamento di categorie particolari di dati.

L. 137/2023: legge 9 ottobre 2023 n. 137 '*Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione'* (c.d. decreto giustizia), che ha anche riformato l'art. 255 del TUA-Testo unico ambientale (d. lgs. 152/2006) introducendo la sanzione penale anche per gli abbandoni di rifiuti da parte dei privati.

Linee guida crittografia: Agenzia per la Cybersicurezza Nazionale e Garante per la protezione dei dati personali '*Guidelines 01/2022 on data subject rights - Right of access*' [Linee guida 1/2022 sui diritti degli interessati. Diritto di accesso]", adottate nella versione definitiva 2.0 il 28 marzo 2023.

Linee guida diritti: EDPB '*Guidelines 01/2022 on data subject rights - Right of access*' [Linee guida 1/2022 sui diritti degli interessati. Diritto di accesso]", adottate nella versione definitiva 2.0 il 28 marzo 2023.

Linee guida DPIA: WP29 '*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del regolamento (UE) 2016/679*', adottate nella versione definitiva il 4 ottobre 2017.

Linee guida DPO: WP29 '*Linee guida sui responsabili della protezione dei dati*', adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017.

Linee guida INAD: AGID *'Linee guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi*

---

[4] Denominazione per esteso: "*Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

[5] Denominazione per esteso: "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*".

o registri professionali o nel registro delle imprese', versione 1.0 del 15 settembre 2021.

Linee guida password: Agenzia per la Cybersicurezza Nazionale e Garante per la Protezione dei Dari Personali *'Linee Guida funzioni crittografiche. Conservazione delle password'*, adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018.

Linee guida profilazione: WP29 *'Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679'*, adottate il 7 dicembre 2023.

Linee guida titolare: EDPB '*Linee guida 7/2020 sul concetto di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*' adottate per la pubblica consultazione il 2 settembre 2020.

Linee guida trasparenza: WP29 '*Linee guida sulla trasparenza ai sensi del regolamento 2016/679*', adottate il 29 dicembre 2017 ed emendate l'11 aprile 2018.

Linee guida videosorveglianza: EDPB '*Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video'*, adottate nella versione 2.0 il 29 gennaio 2020.

Manuale ENISA: '*Manuale sulla sicurezza nel trattamento dei dati personali*' adottato da European Union Agency for Network and Information Security (ENISA) nel dicembre 2017.

Misure minime AGID: circolare 18 aprile 2017, n. 2/2017 '*Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»*'.

Norme nazionali sulla trasparenza: legge 7 agosto 1990 n. 241 '*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*' e successive modificazioni e integrazioni; decreto legislativo 14 marzo 2013 n. 33 '*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*'; FOIA (Freedom of Information Act), introdotto con il decreto legislativo 25 maggio 2016, n. 97 '*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*'.

Preleggi: '*Disposizioni sulla legge in generale*', approvate con Regio Decreto 16 marzo 1942, n. 262, con il quale fu approvato anche il codice civile italiano, come modificato dalla L. 31 maggio 1995 n. 218.

Raccomandazioni videosorveglianza: EDPB '*Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza'*, adottate il 10 novembre 2020.

Statuto dei lavoratori: legge 20 maggio 1970 n. 300 '*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamenti*', uno dei primi in assoluto che disciplina l'attività di videosorveglianza.

Trattato di Lisbona: '*Trattato di Lisbona che modifica il trattato sull'Unione europea e il trattato che istituisce la Comunità europea, firmato a Lisbona il 13 dicembre 2007*', è uno dei trattati dell'Unione Europea, entrato ufficialmente in vigore il 1º dicembre 2009.

TUA: decreto legislativo 3 aprile 2006 n. 152 *'Norme in materia ambientale'* come modificato e aggiornato in ultimo dalla legge 9 ottobre 2023 n. 137.

TUEL: decreto legislativo 18 agosto 2000 n. 267 *'Testo unico delle leggi sull'ordinamento degli enti locali'* come modificato e aggiornato in ultimo dal decreto legislativo 31 marzo 2023 n. 36.

Si è presa visione anche del , approvato con n. del e del **Errore. CampoUnione non è stato trovato nel record intestazione dell'origine dati.** e del **Errore. CampoUnione non è stato trovato nel record intestazione dell'origine dati.** e del FALSO, delle informative rese agli interessati, della documentazione tecnica disponibile sui sistemi di ripresa e delle ulteriori procedure operative trasmesse dal titolare.

A1.5 Elenco degli acronimi

Nel prosieguo del presente documento si utilizzano le seguenti abbreviazioni:

ACN: acronimo di Agenzia per la Cybersicurezza Nazionale, ente di diritto pubblico istituito a tutela degli interessi nazionali nel campo della cybersicurezza, istituita con il decreto legge n. 82 del 14 giugno 2021 e convertito con modificazioni nella legge n. 109 del 4 agosto 2021.

CJEU: acronimo, nelle due lingue ufficiali dell'Unione Europea, di Court of Justice of the European Union (inglese) e Cour de Justice de l'Union européenne (francese), ossia la Corte di giustizia dell'Unione europea, da cui anche l'acronimo CGUE.

DC: acronimo di *Data Controller* che in italiano è il titolare del trattamento dei dati personali (art. 24 par. 1 num. 7 GDPR[6] e art. 2 lett. h lgs. 51/2018[7]) .

DP: acronimo di *Data Processor* che in italiano è il responsabile del trattamento (art. 24 par. 1 num. 8 GDPR[8] e art. 2 lett. i lgs. 51/2018[9]).

DPIA: acronimo di *Data Protection Impact Assessment* ossia valutazione d'impatto sulla protezione dei dati prevista e disciplinata dall'art. 35 GDPR, Linee guida videosorveglianza e dall'art. 23 d. lgs. 51/2018, per i trattamenti di polizia finalizzati alla prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali (art. 2 par. 2 lett. d GDPR, art. 1 c. 2 d. lgs. 51/2018) e la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse (art. 2 p. 2 lett. d GDPR, art. 1 c. 2 d. lgs. 51/2018).

DPO: acronimo di *Data Protection Officer*, termine anglosassone che indica il responsabile per la protezione dei dati, indicato anche con l'acronimo RPD, disciplinato dal regolamento UE 2016/679 (art. 37-39 GDPR) e previsto anche per i trattamenti esclusi dal GDPR (art. 28-30 d. lgs. 51/2018).

DS: acronimo di *Data Subject* che in italiano è l'interessato ossia il soggetto al quale si applica il

---

[6] Reg. (UE) (UE) 2016/679 GDPR, art. 4 (Definizioni): «*1. Ai fini del presente regolamento s'intende per: […] 7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*».

[7] D. lgs. 51/2018 art. 2 (Definizioni): «*1. Ai fini del presente decreto, si applicano le seguenti definizioni:[…] h) titolare del trattamento: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione europea o dello Stato, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione europea o dello Stato;*».

[8] Reg. (UE) (UE) 2016/679 GDPR, art. 4: «*1. Ai fini del presente regolamento s'intende per: […] 8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*».

[9] D. lgs. 51/2018 art. 2: «*1. Ai fini del presente decreto, si applicano le seguenti definizioni:[…] i) responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*».

trattamento dei suoi dati personali (art. 3 par. 2 GDPR[10] e art. 2 lett. a lgs. 51/2018[11]).

EDPB: acronimo di *European Data Protection Board*, tradotto come Comitato Europeo per la Protezione dei Dati, organo costituito dai rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo, massima autorità preposta all'interpretazione e applicazione del regolamento UE 2016/679 GDPR.

GPDP: acronimo di Garante per la Protezione dei Dati Personali, autorità nazionale italiana, istituita sin dalla prima normativa nazionale sulla protezione dei dati personali la legge 675/1996 (art.30) e ribadita con il d. lgs. 101/2018 (art.2-ter d. lgs. 196/2003).

RPD: acronimo di responsabile per la protezione dei dati, si veda quanto detto per il DPO.

WP 29: acronimo di Article 29 Working Party, tradotto come Gruppo di lavoro dell'articolo 29 per la protezione dei dati, era il consiglio della autorità nazionali di vigilanza e protezione dei dati degli Stati membri UE, organismo consultivo indipendente, che prendeva il nome dall'articolo 29 della direttiva 95/46/UE che lo aveva istituito. Dal 25 maggio 2018 è stato sostituito dallo European Data Protection Board (EDPB).

A1.6 Disciplina tecnica di riferimento e responsabilità

Poiché la disciplina giuridica europea (art. 35 GDPR) e le indicazioni per l'applicazione (Linee guida videosorveglianza e Linee Guida DPIA) non forniscono alcun metodo e tantomeno la disciplina tecnica per svolgere la valutazione d'impatto sulla protezione dei dati-DPIA, rimettendo il tutto al principio generale dell' "*accountability*" che consiste nell' "*essere in grado di dimostrare, che il trattamento è effettuato conformemente*" a tutte le norme sulla protezione dei dati (art. 24 par. 1 GDPR[12]), è necessario utilizzare un metodo oggettivo che dimostri l'affidabilità e l'impegno concreto e non meramente formale del titolare del trattamento.

L'utilizzo di semplicissimi software finalizzati alla preliminare valutazione della necessità della DPIA e non già allo svolgimento e alla quantificazione del rischio secondo parametri oggettivi e delle misure di sicurezza, come quello elaborato dall'Autorità nazionale francese Framework CNIL, non dimostra l'accountability e non esclude la responsabilità del titolare del trattamento che è responsabile dell'inadeguatezza della procedura di valutazione d'impatto.

Occorre quindi fare riferimento a discipline tecniche dettagliate e riconosciute a livello internazionale e che consentano:

- definizioni della terminologia e dei concetti di base in maniera univoca (*risk vocabulary*);
- metodi di valutazione e misurazione del rischio standardizzato e oggettivo (*risk evaluation*);
- procedure affidabili di analisi e gestione del rischio (*risk management*).

Altrimenti non avrebbe alcuna affidabilità la valutazione d'impatto sul trattamento dei dati e il titolare del trattamento non potrebbe nemmeno rilevare oggettivamente la sussistenza dell'obbligo o, laddove

[10] Reg. (UE) (UE) 2016/679 GDPR, art. 3 (Ambito di applicazione territoriale): «*2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione,[…]*».

[11] D. lgs. 51/2018 art. 2: «*1. Ai fini del presente decreto, si applicano le seguenti definizioni:[…] a) dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);*».

[12] Reg. (UE) (UE) 2016/679 GDPR, art. 24 (Responsabilità del titolare del trattamento: «*1. […] il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. […]*».

non fosse elevato il rischio, valutare compiutamente l'opportunità di inviare questo documento per l'approvazione preventiva all'autorità garante (art. 36 GDPR[13]).

Quindi il riferimento oggettivo per lo svolgimento della valutazione d'impatto sulla protezione dei dati può essere individuato nelle norme universali di armonizzazione e standardizzazione, definite dall'ente internazionale di standardizzazione ISO-International Organization for Standardization, che è riconosciuto da tutti gli Stati, e in particolare nelle norme che seguono e che sono state utilizzate per il presente documento:

- **ISO Guide 73:2009** "*Risk management vocabulary*", in vigore dal 15/11/2009, che fornisce le definizioni standardizzate dei termini della gestione del rischio per una comprensione reciproca tra tutti gli operatori e un approccio coerente alla descrizione e alla gestione del rischio tra tutti coloro i quali si occupano della gestione;
- **ISO 31000:2018** "*Gestione del rischio - Linee guida*", in vigore dal 17/05/2018, che definisce le indicazioni standardizzate per la gestione di qualsiasi tipo di rischio in tutte le attività, a prescindere dal settore, incluso il processo decisionale a ogni livello;
- **UNI CEI EN IEC 31010:2019** "*Gestione del rischio - Tecniche di valutazione del rischio*", in vigore dal 19/12/2019, che costituisce la guida per la scelta e l'applicazione di tecniche di valutazione del rischio, a supporto dei processi decisionali in tutte le situazioni di incertezza, per valutare e gestire il rischio a prescindere dal contesto e dal settore;
- **ISO/IEC 29134:2023** "*Information technology - Security techniques - Guidelines for privacy impact assessment*", in vigore dall'8 maggio 2023, che fornisce linee guida per svolgere la valutazione d'impatto sulla vita privata, applicabili a tutti i tipi e dimensioni di organizzazioni, comprese le aziende pubbliche e private, gli enti governativi e le organizzazioni senza scopo di lucro.

A1.7 Il metodo standardizzato per la valutazione e gestione del rischio

Per affrontare i rischi in modo sistematico, il normatore ISO-International Organization for Standardization (https://www.iso.org/) ha emesso una serie di norme, la principale delle quali è la ISO 31000.

Partendo da un linguaggio comune in tutte le nazioni e contesti, definito in maniera standardizzata dalla norma ISO 73:2009 "*Risk management vocabulary*" [in italiano Vocabolario della gestione del rischio], i principi di gestione del rischio indicati dalla norma *ISO 31000 "Risk management – Principles and guidelines"* [in italiano Gestione del rischio - Principi e linee guida], arrivata alla nuova revisione del 2018, è stata elaborata dal Comitato Tecnico ISO/TMB "*Risk Management"* e in particolare dalla Commissione Tecnica UNI Sicurezza della società e del cittadino ed è stata approvata dalla Commissione Centrale Tecnica dell'UNI nella prima edizione il 27 ottobre 2010.

Il metodo standardizzato definito in questa norma consente di gestire in maniera uniforme, in modo oggettivo e a livello internazionale, qualsiasi tipo di rischio, sia per conseguenze di tipo positivo che negativo, a prescindere dal settore e dal contesto, definendo un linguaggio comune e un metodo uniforme per la definizione di strategie, decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.

[13] Reg. (UE) (UE) 2016/679 GDPR, art. 36 (Consultazione preventive): «*1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.. […]*».

Questo sistema è applicabile a tutte le tipologie di organizzazioni, pubbliche e private, commerciali o non-profit, associazioni, organi governativi e non, di qualsiasi dimensione e settore, persino agli individui.

Lo scopo è quello di fornire risultati comparabili e oggettivi per la quantificazione e gestione dei rischi, sebbene non certificabili poiché questa normativa è una linea guida.

Per lo svolgimento della presente valutazione d'impatto sulla protezione dei dati personali-DPIA, si sono seguiti i principi della norma ISO 31000:2018, la terminologia definita dalla norma ISO 73:2009 e il metodo indicato dalla norma ISO/IEC 29134:2023.

Questo approccio consente di individuare i rischi e quantificarli in maniera oggettiva e riconosciuta a livello internazionale, garantendo e dimostrando il rispetto del principio di accountability (art. 24 c. 1 GDPR) che è alla base non solo della valutazione d'impatto in via generale (art. 35 GDPR), in particolare nel caso di trattamenti con l'impiego di strumenti di videosorveglianza (Linee guida videosorveglianza) ma, come si illustrerà in seguito, dell'intera disciplina del GDPR.

Di seguito è riportato lo schema riassuntivo generale dei principi e dei processi standardizzati ISO che sono stati citati e che sono seguiti in tutte le fasi del presente documento.

Sezione A2 -Inquadramento della DPIA

A2.1 Lo scopo della valutazione d'impatto

La valutazione d'impatto sulla protezione dei dati è una procedura, nota anche con l'acronimo PIA (*Privacy Impact Assessment*) o DPIA (*Data Privacy Impact Assessment*) e quest'ultimo acronimo si utilizzerà di seguito per indicare la procedura, è prevista dall'art. 35 del regolamento (UE) 2016/679 e dall'art. 23 del d. lgs. 51/2018 per i soli trattamenti finalizzati alla prevenzione, indagine, accertamento, perseguimento di reati, esecuzione di sanzioni penali, prevenzione e salvaguardia della sicurezza pubblica (art. 1 d. lgs. 51/2018 e art. 2 par. 2 lett. d GDPR).

Il processo di valutazione d'impatto può riguardare sia un singolo trattamento e sia più trattamenti che presentino analogie per natura, ambito, finalità e rischi[14].

Questa procedura ha lo scopo di descrivere un trattamento di dati per valutarne la necessità e la proporzionalità così come tutti gli altri principi fondamentali della normativa vigente. Dalla descrizione del trattamento ne consegue la valutazione del rischio e la sua misurazione, quindi su questa conoscenza si possono predisporre idonee misure per affrontare e ridurre i rischi a livelli accettabili e sostenibili, con una gestione consapevole e responsabile.

Proprio la responsabilizzazione, o "*accountability*" come viene definito nel testo originale del GDPR, è il principio cardine della normativa europea sulla protezione dei dati personali e consiste nell' "*essere in grado di dimostrare, che il trattamento è effettuato conformemente*" a tutte le norme sulla protezione dei dati (art. 24 par. 1 GDPR[15]). Quindi la valutazione d'impatto sulla protezione dei dati-DPIA è uno strumento importante per il titolare del trattamento perché lo aiuta a rispettare le prescrizioni normative, evidenziando le situazioni di illegittimità che non siano già state rilevate e approfondendo situazioni d'incertezza nell'applicazione delle norme, e lo supporta nel percorso di conformità suggerendo e valutando le misure di attenuazione del rischio nei tempi accettabili e, in questo modo, costituisce una dimostrazione di conformità del trattamento alla disciplina sulla protezione dei dati, ossia di accountability, come richiede la normativa europea (art. 24 par. 1 GDPR).

A2.2 Obbligo della valutazione d'impatto

A2.2.1 CASI IN CUI È RICHIESTA LA DPIA NEI TRATTAMENTI SOGGETTI AL GDPR

La valutazione d'impatto sulla protezione dei dati-DPIA è obbligatoria, come regola generale, in tutti i casi nei quali un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 par. 1 GDPR[16], considerando 85[17]) a causa di:

---

[14] Reg. (UE) (UE) 2016/679 GDPR, art. 35: «*1. [...]Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi [...]*».

[15] Reg. (UE) (UE) 2016/679 GDPR, art. 24: «*1. [...] il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. [...]*».

[16] Reg. (UE) 2016/679 GDPR, art. 35: «*1. 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,[...]*».

[17] Reg. (UE) 2016/679 GDPR, considerando 85: «*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a*

- *implementazione di nuove tecnologie*;
- *natura, oggetto, contesto o finalità del trattamento*.

Lo stesso GDPR cita anche alcune ipotesi specifiche che rendono sempre obbligatoria la DPIA che sono (art. 35 par. 3 GDPR[18]):

- *valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato*, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (art. 35 par. 3 lett. a GDPR);
- *trattamento, su larga scala, di categorie particolari di dati personali* (art. 9 GDPR) ovvero di dati relativi a condanne penali (art. 10 GDPR) ovvero a reati (art. 35 par. 3 lett. b GDPR);
- *sorveglianza sistematica su larga scala di una zona accessibile al pubblico* (art. 35 par. 3 lett. c GDPR), in questa ipotesi rientrano in particolare tutti i trattamenti che impieghino sistemi di ripresa di immagini fisse e in movimento (Linee guida videosorveglianza).

A2.2.2 ESTENSIONE DELL'OBBLIGO DELLA DPIA ANCHE AI TRATTAMENTI ESCLUSI DAL GDPR

I trattamenti di dati finalizzati ad attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvaguardia e prevenzione di minacce alla sicurezza pubblica eseguito dalle competenti autorità, noti in ambito europeo anche come "*Law Enforcement Purposes*" da cui l'acronimo LEP, sono esclusi dall'ambito di applicazione materiale del regolamento (UE) 2016/679 (art. 2 par. 2 lett. d GDPR[19] e art. 1 d. lgs. 51/2018[20]) e sono disciplinati dalla c.d. "*direttiva di polizia*", nota con l'acronimo LED da "*Law Enforcement Directive*", che è la direttiva (UE) 2016/680[21], recepita in Italia con il decreto legislativo 18 maggio 2018, n. 51.

Anche questi trattamenti sono soggetti all'obbligo di valutazione d'impatto sulla protezione dei dati-DPIA quando, per l'uso di nuove tecnologie e per la loro natura, per l'ambito di applicazione, per il

---

conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.».

[18] Reg. (UE) 2016/679 GDPR, art. 35 «*3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*».

[19] Reg. (UE) 2016/679 GDPR, art. 2 (Ambito di applicazione materiale): «*2. Il presente regolamento non si applica ai trattamenti di dati personali:...omissis… d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.*».

[20] D. lgs. 51/2018 art. 1 (Oggetto e ambito di applicazione): «*1. Il presente decreto attua nell'ordinamento interno le disposizioni della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio. 2. Il presente decreto si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti a fini 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.*».

[21] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio d'Europa, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (c.d. direttiva di polizia).

contesto e per le finalità, presenta un rischio elevato (considerando 53 Direttiva europea 2016/680[22]) per i diritti e le libertà delle persone fisiche (art. 23 d. lgs. 51/2018).

Rientrano in questo ambito i trattamenti per le finalità di polizia giudiziaria (art. 97 c.p.p.) e per le attività ausiliarie di pubblica sicurezza (art. 5 l. 65/1986) svolti dalla Polizia Locale.

A2.2.3 ESCLUSIONE DELLA NECESSITÀ DELLA DPIA SECONDO LE PRESCRIZIONI DEL GDPR.

La DPIA è esclusa quando si verificano contemporaneamente le seguenti condizioni (art. 35 par. 10 GDPR[23]):

1. **Finalità del trattamento di interesse pubblico** e specificatamente in uno dei seguenti casi:
   a. adempimento di un obbligo legale al quale è soggetto il titolare del trattamento;
   b. esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
2. **Disciplina normativa esplicita della finalità di interesse pubblico** contenuta in un atto normativo Europeo o dello Stato membro al quale il titolare del trattamento è soggetto.
3. **Sia già stata eseguita una DPIA nell'ambito di una valutazione d'impatto generale** nel contesto dell'adozione della disciplina giuridica di cui al punto precedente.

A2.2.4 ULTERIORI OBBLIGHI DI DPIA INTRODOTTI DAL GARANTE ITALIANO

L'autorità nazionale di controllo, nel caso dell'Italia il Garante per la protezione dei dati personali, ha il potere e la facoltà di prevedere delle specifiche tipologie di trattamento per i quali è obbligatoria l'adozione del DPIA (art. 35 par. 4 GDPR[24]), in questi casi ha l'obbligo di pubblicare il provvedimento e comunicarlo al comitato europeo per la protezione dei dati (art. 35 par. 6 GDPR[25]) che era Gruppo di lavoro articolo 29 o Article 29 Working Party (noto anche con l'acronimo WP29), fino al 25 maggio del 2018 (data di entrata in vigore del RGPD) e aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali, ed è stato sostituito in seguito dal Comitato europeo per la protezione dei dati (art. 68 GDPR).

---

[22] Direttiva (UE) 2016/680, considerando 53: «*La tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni della presente direttiva. L'attuazione di tali misure non dovrebbe dipendere unicamente da considerazioni economiche. Al fine di poter dimostrare la conformità con la presente direttiva, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che aderiscano in particolare ai principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita. Se il titolare del trattamento ha effettuato una valutazione d'impatto sulla protezione dei dati ai sensi della presente direttiva, è opportuno prenderne in considerazione i risultati in fase di sviluppo delle misure e delle procedure suddette. Le misure potrebbero consistere, tra l'altro, nell'utilizzo della pseudonimizzazione il più presto possibile. L'utilizzo della pseudonimizzazione ai fini della presente direttiva può essere strumentale per agevolare, in particolare, la libera circolazione dei dati personali all'interno dello spazio di libertà, sicurezza e giustizia.*».

[23] Reg. (UE) 2016/679 GDPR, art. 35: «*10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.*».

[24] Reg. (UE) 2016/679 GDPR, art. 35: «*4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.*».

[25] Reg. (UE) 2016/679 GDPR, art. 35: «*6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.*».

Per specificare nel dettaglio e dare maggiore certezza è intervenuto il provvedimento del Garante per la Protezione dei Dati Personali che con la delibera 11 ottobre 2018, n. 467 "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35, comma 4, del regolamento (UE) n. 2016/679*", che ha attuato le indicazioni del Article 29 Working Party del 2017 fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

In questo modo si è stabilito l'obbligo di DPIA nei casi in cui ricorrano almeno due di questi criteri anche se il titolare può deciderla anche quando ne ricorra uno solo in funzione delle implicazioni sulla sicurezza:

- **trattamenti valutativi o di scoring**, compresa la profilazione;
- **decisioni automatizzate** che producono significativi effetti giuridici (es. assunzioni, concessione di prestiti, stipula di assicurazioni);
- **monitoraggio sistematico**, come avviene sempre con l'impiego di strumenti di videosorveglianza ossia con sistemi di ripresa di immagini fisse o mobili;
- **trattamento di categorie particolari di dati personali**, come sono definiti (art. 9 GDPR e art. 7 d. lgs. 51/2018) e quindi i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici e biometrici e quelli relativi alla salute o alla vita o all'orientamento sessuale;
- **trattamento di dati personali su larga scala**, come avviene in tutti i casi di videosorveglianza o anche di rilevamento di targhe di veicoli;
- **combinazione o raffronto di insiemi di dati** derivanti da due o più trattamenti svolti per differenti finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene ad esempio con i big data);
- **dati relativi a soggetti vulnerabili**, come ad esempio minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.;
- **utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative**, come nel caso di riconoscimento facciale, devices IOT-internet of things, sistemi di localizzazione, ecc.;
- **trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto** o di avvalersi di un servizio o di un contratto, come ad esempio i sistemi di scoring utilizzati dalle banche accedendo alle centrali rischio per stabilire la concessione di finanziamenti.

A2.2.5 CASI DI ESCLUSIONE DELLA DPIA STABILITI DAL GARANTE

Il Garante per la protezione dei dati personali, secondo quanto previsto dal Regolamento Europeo (art. 35 par. 5 GDPR[26]), ha stabilito che la DPIA non è necessario per i trattamenti che:

- non presentano rischio elevato per i diritti e le libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata svolta una DPIA;

[26] Reg. (UE) 2016/679 GDPR, art. 35: «*5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.*».

- sono stati già sottoposti a verifica da parte di un'autorità di controllo prima del maggio 2018 e le cui condizioni (es. oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo del trattamento per i quali non è necessaria provvedere alla DPIA;
- fanno riferimento a norme o regolamenti UE o di uno Stato membro per la cui definizione è stata condotta una DPIA.

A2.3 Chi deve svolgere la DPIA

Il titolare del trattamento ha la responsabilità, secondo il principio di accountability, di valutare la necessità di svolgere la Valutazione d'impatto-DPIA (art. 35 par. 1 GDPR[27] e art. 23 c. 1 d. lgs. 51/2018[28]) e, laddove si renda necessaria, l'obbligo di provvedere alla realizzazione sovrintendendo sempre ogni fase, pur se la realizzazione materiale sia demandata ad altro soggetto (consulente esterno o dipendente).

Nella decisione sulla realizzazione e nello svolgimento si consulta con il DPO/RPD (art. 35 par. 2 GDPR[29]) inoltre, se il trattamento lo richiede, può acquisire pareri di esperti, tecnici e in particolare del responsabile della sicurezza dei sistemi informativi (noto anche come *Chief Information Security Officer*, acronimo CISO) e del responsabile IT (acronimo di *Information Technology*), laddove presenti, da allegare alla DPIA.

Il titolare può acquisire il parere del DPO (art. 39 par. 1 lett. c GDPR), degli interessati o dei loro rappresentanti purché, il parere di questi ultimi non pregiudichi gli interessi del Comune di Santeramo in Colle e purché non si mettano a rischio i trattamenti stessi che si vogliono valutare con la DPIA (art. 35 par. 9 GDPR[30]).

A2.4 Aggiornamento della valutazione d'impatto

La DPIA non è un documento statico ma proprio per le sue finalità generali richiede un processo costante di verifica ed eventuale aggiornamento perlomeno quando insorgono variazioni del rischio, secondo il contesto e le evoluzioni tecnologiche, ovvero mutino o si evolvano le attività relative al trattamento.

In questi casi il titolare del trattamento procede a un riesame per valutare se dalle variazioni delle procedure del trattamento che sono intervenute e/o dalle mutate condizioni del contesto ne scaturisca un pregiudizio, anche solo potenziale, sulla sicurezza del trattamento dei dati personali e se le previsioni contenute nella presente valutazione d'impatto-DPIA siano ancora valide e attuali (art. 35 par. 11 GDPR e art. 15 d. lgs. 51/2018).

---

[27] Reg. (UE) 2016/679 GDPR, art. 35: «*1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*».

[28] D. lgs. 51/2018 art. 23 (Valutazione d'impatto sulla protezione dei dati): «*1. Se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali.*».

[29] Reg. (UE) 2016/679 GDPR, art. 35: «*2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.*».

[30] Reg. (UE) 2016/679 GDPR, art. 35: «*9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.*».

Considerata la struttura del trattamento mediante i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale oggetto della presente valutazione d'impatto, le possibili evoluzioni, incluse quelle eventualmente previste e tutte quelle che ci si aspettino che possano avvenire, la necessità di manutenzione e l'usura prevista per il sistema, le fonti e il livello di rischio, si indica in via generale la necessità della revisione entro 180 giorni/semestrale, pertanto la presente valutazione scade il 3/2/2027 salvo che mutate condizioni del contesto valutato o variazioni del rischio rendano necessaria la revisione anticipata.

A2.5 I principi di valutazione del trattamento

La valutazione d'impatto sulla protezione dei dati-DPIA deve informarsi ai valori e ai criteri generali del trattamento dei dati contenuti nel GDPR e in particolare verificare che siano attuati i principi di:

- *liceità e correttezza* (art. 5 par. 1 lett. a GDPR e art. 3 c. 1 lett. a d. lgs. 51/2018);
- *trasparenza* (art. 5 par. 1 lett. a GDPR);
- *limitazione delle finalità* (art. 5 par. 1 lett. b GDPR e art. 3 c. 1 lett. b d. lgs. 51/2018);
- *minimizzazione dei dati*, (art. 25 par. 2 lett. c GDPR e art. 3 c. 1 lett. c d. lgs. 51/2018);
- *esattezza* (art. 5 par. 1 lett. d GDPR e art. 3 c. 1 lett. c d. lgs. 51/2018);
- *diritto all'oblio* (art. 5 par. 1 lett. e GDPR);
- *integrità e riservatezza* (art. 5 par. 1 lett. f GDPR e art. 3 c. 1 lett. f d. lgs. 51/2018);
- *responsabilizzazione* (art. 5 par. 2 GDPR).

A2.5.1 PRINCIPI DI LICEITÀ, CORRETTEZZA E TRASPARENZA

I principi di liceità, correttezza e trasparenza nella gestione dei dati personali dell'interessato sono fondamentali per tutti i trattamenti (art. 5 par. 1 lett. a GDPR[31]) e anche per quelli esclusi dal campo di applicazione del GDPR (art. 3 c. 1 lett. a d. lgs. 51/2018[32]) con la sola esclusione, dato il particolare contesto delle indagini di polizia, del principio di trasparenza.

Il principio di correttezza va a sostituire il principio di lealtà precipuo della vecchia normativa nella quale dominava un rapporto tra il titolare e l'interessato mentre oggi l'impegno è esteso all'intera società nella quale tutti noi viviamo e esplichiamo i nostri diritti e doveri, per cui il trattamento deve essere corretto, così garantendo all'intera collettività che il trattamento non ponga a rischio i dati personali.

La definizione del principio di correttezza è stata formulata già dal Gruppo di lavoro articolo 29 o Article 29 Working Party (noto anche con l'acronimo WP29), sostituito oggi dall'European Data Protection Board (noto anche con l'acronimo EDPB), che è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati, con riferimento alla chiarezza e trasparenza delle informative, sostenendo la necessità che l'informazione fornita all'interessato debba essere tale da far comprendere in modo adeguato, "*le modalità con cui i dati sono raccolti, utilizzati e consultati grazie*

[31] Reg. (UE) 2016/679 GDPR, art. 5 (Principi applicabili al trattamento di dati personali): «*1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»)…*».

[32] D. lgs. 51/2018 art. 3 (Principi applicabili al trattamento di dati personali): «*1. I dati personali di cui all'articolo 1, comma 2, sono: a) trattati in modo lecito e corretto;...omissis…* ».

ad informazioni e comunicazioni facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro" (art. 12 par. 1 GDPR[33]) e anche le conseguenze.

Quindi, il principio di liceità e correttezza è funzionale e rafforzativo dell'obbligo di trasparenza del trattamento nei confronti degli interessati che rappresenta un vero e proprio diritto dell'interessato.

Il punto di partenza della DPIA è la valutazione della documentazione complessiva relativa al trattamento dei dati e in particolare dell'informativa resa agli interessati.

A2.5.2 PRINCIPIO DI LIMITAZIONE DELLE FINALITÀ

I dati personali, per tutte le finalità (art. 5 par. 1 lett. b GDPR[34]), anche per quelle c.d. di polizia (art. 3 c. 1 lett. b d. lgs. 51/2018[35]), devono essere raccolti per finalità determinate, esplicite e legittime, secondo un principio generale di necessità e proporzionalità che deve applicarsi a tutte le informazioni relative alle persone fisiche e quindi la valutazione della DPIA deve escludere che possano esserci dei trattamenti indiscriminati.

Il titolare del trattamento deve stabilire quindi, prima dell'inizio del trattamento, in maniera precisa e tassativa, evitando formulazioni generiche o illimitate, gli scopi in base ai quali ha intenzione di raccogliere e trattare i dati personali e deve limitarsi alle finalità che ha comunicato all'interessato prima dell'inizio della raccolta dei dati, nei casi previsti (art. 13 e 14 GDPR) e quindi del trattamento.

Ciò implica che se alcuni dei dati personali o se i dati personali di alcuni soggetti non servono per le finalità del trattamento, essi non devono neppure essere raccolti e la DPIA deve quindi verificare che ciò non avvenga nel processo dell'intero trattamento.

A2.5.3 PRINCIPIO DI MINIMIZZAZIONE DEI DATI

Il principio di minimizzazione dei dati parte dall'idea fondamentale che il titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, pertanto per tutte le finalità (art. 5 par. 1 lett. c GDPR[36] e art. 3 c. 1 lett. c d. lgs. 51/2018[37]), i dati devono essere trattati con:

- *adeguatezza*, vale a dire proporzionalità rispetto alle finalità per la quale sono raccolti;
- *pertinenza* rispetto alle finalità precedentemente definite;
- *limitazione* a quanto necessario al raggiungimento delle finalità per i quali sono trattati.

---

[33] Reg. (UE) 2016/679 GDPR, art. 12 (Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato): «*1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.*».

[34] Reg. (UE) 2016/679 GDPR, art. 5: «*1. I dati personali sono:[...]b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità...*».

[35] D. lgs. 51/2018 art. 3: «*1. I dati personali di cui all'articolo 1, comma 2, sono:...omissis… b) raccolti per finalità determinate, espresse e legittime e trattati in modo compatibile con tali finalità;...omissis…* ».

[36] Reg. (UE) 2016/679 GDPR, art. 5: «*1. I dati personali sono:[...] c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);[...]*».

[37] D. lgs. 51/2018 art. 3: «*1. I dati personali di cui all'articolo 1, comma 2, sono:...omissis… c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati;...omissis…* ».

Dunque i dati raccolti devono essere adeguati e pertinenti rispetto al fine che si intende perseguire, ed essi non possono essere raccolti in misura maggiore a quella necessaria.

In sostanza si stabilisce l'obbligo di verificare che per le esigenze del trattamento siano raccolti e gestiti il minor quantitativo di dati possibili.

La DPIA, per questo fine, deve conoscere l'estensione dei trattamenti e valutare l'effettiva necessità dell'estensione della base di dati trattati rispetto alle finalità.

A2.5.4 PRINCIPIO DI ESATTEZZA DEI DATI

I dati trattati debbano essere esatti qualunque sia la finalità del trattamento e, se necessario, aggiornati (art. 5 par. 1 lett. d GDPR[38] e art. 3 c. 1 lett. d d. lgs. 51/2018[39]).

Il titolare, inoltre, deve prendere tutte le misure ragionevoli per cancellare o rettificare tempestivamente quelli che non sono più esatti e, laddove non rilevi errori di sua iniziativa, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, può chiedere anche l'integrazione dei dati personali incompleti fornendo, eventualmente, una dichiarazione integrativa (art. 16 GDPR[40]).

La DPIA, a questo scopo, deve verificare le misure adottate e i sistemi di verifica per garantire la correttezza dei dati trattati.

A2.5.5 DIRITTO ALL'OBLIO

Il diritto all'oblio, inizialmente riconosciuto soltanto a livello giurisprudenziale, sia in campo europeo che nazionale, è stato recepito e disciplinato anche nella normativa europea sulla protezione dei dati.

Può essere definito come l'interesse di un singolo a essere dimenticato e consiste, quindi, nell'obbligo automatico di eliminazione dei trattamenti quando vengono meno la finalità per cui sono trattati, è espressamente riconosciuto quando si verifichino le seguenti condizioni (art. 17 GDPR[41]):

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati (art. 17 par. 1 lett. a GDPR);
2. l'interessato revoca il consenso su cui si basa il trattamento (art. 17 par. 1 lett. b GDPR);

---

[38] Reg. (UE) 2016/679 GDPR, art. 5: «*1. I dati personali sono:[...]d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);[...]*».

[39] D. lgs. 51/2018 art. 3 «*1. I dati personali di cui all'articolo 1, comma 2, sono:...omissis… d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;...omissis…* ».

[40] Reg. (UE) 2016/679 GDPR, art. 16 (Diritto di rettifica): «*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.*».

[41] Reg. (UE) 2016/679 GDPR, art. 17 (Diritto alla cancellazione-"diritto all'oblio"): «*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.*».

3. l'interessato si oppone al trattamento nei casi previsti (art. 17 par. 1 lett. c GDPR);
4. i dati personali sono stati trattati illecitamente (art. 17 par. 1 lett. d GDPR);
5. sussiste un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro per cancellare i dati personali (art. 17 par. 1 lett. e GDPR);
6. dati raccolti relativamente all'offerta di servizi della società dell'informazione (art.17 par. 1 lett. f GDPR).

In tutti questi casi il titolare del trattamento è obbligato a cancellare ogni dato, anche quelli resi eventualmente pubblici secondo la tecnologia disponibile, e in questi casi informerà anche gli altri titolari del trattamento che siano in possesso dei dati personali degli interessati che hanno richiesto la cancellazione affinché provvedano a eliminare i propri trattamenti e cancellino qualsiasi link o copia (art. 17 par. 2 GDPR[42]).

Nell'esatto momento in cui non è più giustificato il trattamento secondo i principi che si sono indicati in precedenza è obbligatorio eliminare o rendere anonimi i dati (art. 5 par. 1 lett. e GDPR[43]), pertanto il procedimento oggetto della verifica della DPIA deve valutare che sussista un sistema automatizzato che, prescindendo dalla richiesta dell'interessato e/o dalla revoca del consenso, laddove esso sia il fondamento giuridico del trattamento, elimini il trattamento quando si verifichino queste condizioni.

L'eliminazione può essere sostituita dall'anonimizzazione dei dati per scopi di archiviazione nel pubblico interesse, di ricerca scientifica o storica ovvero a fini statistici.

Il diritto all'oblio è espressamente escluso in casi tassativamente previsti e specificatamente quando il trattamento si rende necessario:

1. per l'esercizio del diritto alla libertà di espressione e di informazione (art. 17 par. 3 lett. a GDPR)[44];
2. per l'adempimento di un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 17 par. 3 lett. b GDPR)[45]; ;
3. per motivi di pubblico interesse nella sanità pubblica (art. 17 par. 3 lett. c GDPR)[46]; ;

---

[42] Reg. (UE) 2016/679 GDPR, art. 17: «*2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.*».

[43] Reg. (UE) 2016/679 GDPR, art. 5: «*1. I dati personali sono:[...]e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);[...]*».

[44] Reg. (UE) 2016/679 GDPR, art. 17: «*3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione.*».

[45] Reg. (UE) 2016/679 GDPR, art. 17: «*3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:[...] b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;[...]*».

[46] Reg. (UE) 2016/679 GDPR, art. 17: «*3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:[...]c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;[...]* ».

4. a fini di archiviazione e di statistica nel pubblico interesse, di ricerca scientifica o storica (art. 17 par. 3 lett. d GDPR)[47];
5. in ambito giudiziario per l'esercizio o la difesa di un diritto (art. 17 par. 3 lett. e GDPR)[48].

Anche i *LEP-Law Enforcement Purposes*, ossia i trattamenti per finalità di polizia esclusi dall'applicazione del GDPR (art. 2 par. 2 lett. d GDPR e art. 1 D.lgs. 51/2018), sono soggetti al diritto all'oblio disponendosi che essi siano "*conservati con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico*" (art. 3 par. 1 lett. e d. lgs. 51/2018).

A2.5.6 PRINCIPIO DI INTEGRITÀ E RISERVATEZZA

Il principio di integrità e riservatezza prevede che i dati devono essere sempre trattati in modo da garantirne una sicurezza adeguata (art. 5 par. 1 lett. f GDPR[49]).

Il titolare del trattamento ha l'obbligo quindi di adottare tutte le misure di sicurezza tecniche e organizzative adeguate al fine di proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro sottrazione, perdita, distruzione, danni accidentali, ossia da tutte quelle ipotesi che configurerebbero un data breach (art. 34 GDPR[50]).

La DPIA quindi deve verificare preventivamente che la sicurezza sia garantita nei confronti dei dati lungo l'intero ciclo del trattamento e, laddove non sia possibile eliminare del tutto il rischio che siano adottate tutte le misure disponibili, sul piano fisico e tecnologico, per minimizzare il rischio.

A2.5.7 PRINCIPIO DI RESPONSABILITÀ

Il principio di accountability (art. 5 par. 2 GDPR[51]) termine del testo originale inglese del GDPR è stato tradotto come "responsabilizzazione" e definito come l'obbligo posto in capo al titolare del trattamento di essere competente, e quindi concretamente in grado, di garantire i principi generali del trattamento indicati in precedenza e altresì di poterlo comprovare.

Da ciò ne consegue l'obbligo di una gestione del trattamento "responsabile" che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento e dalla legislazione nazionale e la responsabilizzazione del titolare del trattamento a cui viene affidato sia il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali in considerazione della realtà produttiva nella quale opera.

---

[47] Reg. (UE) 2016/679 GDPR, art. 17: «*3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:[...]d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;[...]*».

[48] Reg. (UE) 2016/679 GDPR, art. 17: «*3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:[...]e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.*».

[49] Reg. (UE) 2016/679 GDPR, art. 5: «*1. I dati personali sono:[...]f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)[...]*».

[50] Reg. (UE) 2016/679 GDPR, art. 34 (Notifica di una violazione dei dati personali all'autorità di controllo): «*1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*».

[51] Reg. (UE) 2016/679 GDPR, art. 5: «*2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*».

La DPIA quindi deve valutare anche l'impegno progettuale, nell'ottica del principio di privacy by design, e l'azione concreta del titolare, nell'attuazione del concetto di privacy by default, rispetto l'organizzazione della gestione di tutti i trattamenti svolti.

A2.6 Contenuti della valutazione d'impatto

A2.6.1 CONTENUTI GENERALI

La DPIA deve contenere, oltre la generale e complessiva valutazione dell'impatto del trattamento sulle libertà e sui diritti delle persone fisiche, alcune parti ritenute inderogabilmente essenziali (art. 35 par. 7 GDPR, art. 23 c. 2 d. lgs. 51/2018[52]):

- **descrizione generale del trattamento complessivo**, contenente la descrizione sistematica del trattamento complessivo e delle singole procedure che lo compongono, delle finalità e, se possibile, l'esplicazione degli interessi legittimi perseguiti dal titolare (art. 35 par. 7 lett. a GDPR[53], art. 23 c. 2 d. lgs. 51/2018);
- **valutazione della proporzionalità**, di tutti i singoli trattamenti valutati in relazione alle loro finalità (art. 35 par. 7 lett. b GDPR[54]).
- **risk analysis**, ossia una valutazione dettagliata dei rischi derivanti dal trattamento che possano sui diritti e sulle libertà degli interessati (art. 35 par. 7 lett. c GDPR[55], art. 23 c. 2 d. lgs. 51/2018);
- **progetto operativo**, contenente il dettaglio delle misure di sicurezza predisposte per affrontare i rischi sulla sicurezza dei dati personali nella misura più efficace in modo da poter dimostrare la conformità del trattamento alle precisioni del Regolamento Europeo (art. 35 par. 7 lett. d GDPR[56], art. 23 c. 2 d. lgs. 51/2018).

A2.6.2 CONTENUTI DELLA VALUTAZIONE PER FINALITÀ DI POLIZIA

La presente DPIA valuta anche i trattamenti di dati finalizzati ad attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvaguardia e prevenzione di minacce alla sicurezza pubblica eseguito dalle competenti autorità, i trattamenti di polizia-LEP devono contenere specificatamente (art. 23 c. 2 d. lgs. 51/2018[57]):

---

[52] D. lgs. 51/2018 art. 23 (Valutazione d'impatto sulla protezione dei dati): «*2. La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto.*».

[53] Reg. (UE) 2016/679 GDPR, art. 35: «*7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;[...]*».

[54] Reg. (UE) 2016/679 GDPR, art. 35: «*7. La valutazione contiene almeno:[...]b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;[...]*».

[55] Reg. (UE) 2016/679 GDPR, art. 35: «*7. La valutazione contiene almeno:[...] c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1 [ndr art.35 c.1: «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,[...]*».

[56] Reg. (UE) 2016/679 GDPR, art. 35: «*7. La valutazione contiene almeno:[...] d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*».

[57] D. lgs. 51/2018 art. 23 (Valutazione d'impatto sulla protezione dei dati): « *2. La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per*

- **descrizione generale dei trattamenti** in atto e di quelli previsti;
- **valutazione dei rischi** per i diritti e le libertà degli interessati;
- **le garanzie, le misure di sicurezza e i meccanismi** per garantire la protezione dei dati personali e il rispetto delle norme.

Nulla vieta che una sola valutazione d'impatto possa valutare complessivamente sia i trattamenti per le finalità ricomprese nella disciplina del GDPR e sia i trattamenti che ne sono esclusi, disciplinati dalla direttiva di polizia-LED recepita dal decreto legislativo 51/2018, purché essi siano valutati distintamente in funzione delle specifiche finalità e dei differenti requisiti imposti dalle norme.

affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto.».

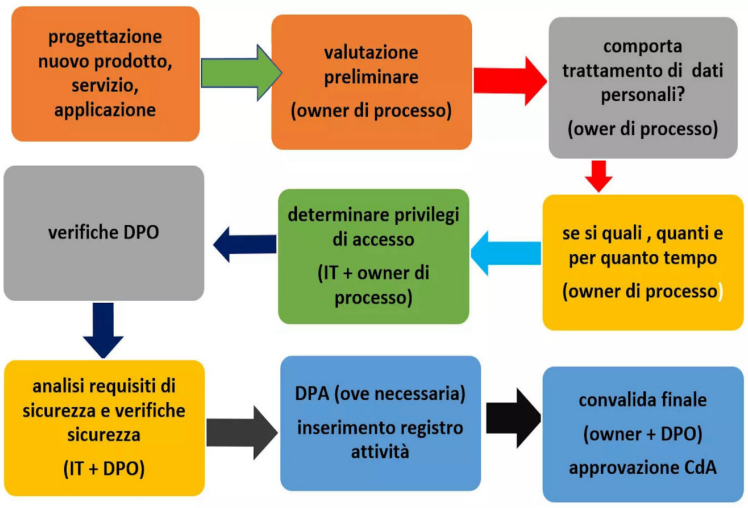
Sezione A3 -Procedura per la misurazione e gestione del rischio

A3.1 Metodologia per la risk evaluation e risk management

A3.1.1 PREMESSA ALLA QUANTIFICAZIONE E QUALIFICAZIONE DEL RISCHIO

La vigente normativa europea per la protezione dei dati assegna al titolare del trattamento l'obbligo di svolgere la valutazione d'impatto nei casi in cui l'adozione di nuove tecnologie nei trattamenti possano presentare rischi per i diritti e le libertà delle persone fisiche ovvero in alcune ipotesi specifiche come in tutti i casi in cui si impieghino sistemi di videosorveglianza (lett. 2.1 7 Linee guida videosorveglianza[58]), ma non definisce le modalità tecniche di svolgimento e i parametri per la misurazione del rischio.

Ciò non implica che il titolare abbia una discrezionalità tale che gli consenta di adempiere in qualsiasi modo ritenga opportuno o, peggio, che possa limitarsi al mero adempimento formale, perché egli deve adempiere all'obbligo della valutazione d'impatto sulla protezione dei dati personali nel rispetto del principio di accountability ossia di responsabilizzazione e rendicontazione in capo al titolare rispetto la correttezza del trattamento eseguito (art. 24 par. 1 GDPR), l'adozione di misure efficaci per la protezione dei dati personali gestiti e la corretta e integrale applicazione del regolamento "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*" e deve "*…essere in grado di dimostrare*" e quindi rendicontare le sue scelte e gli atti che ha predisposto e adottato.



Questo principio vale anche per i trattamenti di dati finalizzati ad attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvaguardia e prevenzione di minacce alla sicurezza pubblica eseguito dalle competenti autorità, che costituiscono quelli che si definiscono trattamenti di polizia o Law Enforcement Procedures (LEP), poiché è espressamente previsto che "*Il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del presente decreto*" (art. 15 c. 1 d. lgs. 51/2018) con la sola differenza che in questi casi non è previsto il principio dell'accountability e quindi non si richiede di "*…essere in grado di dimostrare*" e quindi rendicontare la legittimità del trattamento e la logica delle scelte sul quale si è basato.

[58] EDPB-European Data Protection Board. Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Versione 2.0 29 gennaio 2020, punto 2 Ambito di applicazione «*7. La sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi [...]. Questa attività comporta la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone che entrano nello spazio monitorato identificabili in base al loro aspetto o ad altri elementi specifici. [...] Ciò si riflette nel RGPD all'articolo 35 paragrafo 3 lettera c) che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di sorveglianza sistematica su vasta scala di un'area accessibile al pubblico [...]*».

Corollari di questo principio sono quelli di **privacy by design** (art. 25 par. 1 GDPR[59] e art. 16 c. 1 d. lgs. 51/2018[60]) e **privacy by default** (art. 25 par. 2 GDPR[61] e art. 16 c. 2 d. lgs. 51/2018[62]).

Quindi per assolvere correttamente agli obblighi imposti per la valutazione d'impatto-DPIA si deve:

- svolgere correttamente l'analisi dell'impatto dei trattamenti sulle libertà e sui diritti degli interessati impiegando metodi standardizzati a livello internazionale e non semplicemente utilizzando dei software o delle procedure compilative meramente formali;
- misurare il rischio in maniera oggettiva e riscontrabile, astenendosi dal dare giudizi meramente discrezionali e soggettivi;
- individuare misure specifiche per attenuare i rischi con modalità esplicite e tempi definiti;
- laddove residui un rischio elevato si deve inviarla in valutazione preventiva all'Autorità garante (art. 35 par. 1 GDPR[63]).

Per assolvere in maniera oggettiva e dimostrabile a questi obblighi si deve fare riferimento a procedure scientifiche validate a livello internazionale come sono le norme dettate dall'ISO-International Organization for Standardization e la presente valutazione d'impatto sul trattamento dei dati le utilizza in tutto lo svolgimento.

A3.1.2 DEFINIZIONE DI RISCHIO

La definizione di rischio si trova standardizzata nelle norme ISO che lo definiscono come "*l'effetto dell'incertezza sugli obiettivi*", considerando che "*un effetto è uno scostamento da quanto atteso, positivo o negativo che sia*" (ISO Guide 73: 2009 1.1, ISO 31000:2018 2.1).

Il GDPR considera il rischio come il rapporto tra la stima della probabilità che accada una lesione ai diritti tutelati e la stima delle conseguenze (cap. III par. 2 Linee guida DPIA).

---

[59] Reg. (UE) (UE) 2016/679 GDPR, art.25 (Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita): «*1. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*».

[60] D. lgs. 51/2018 art. 16 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita): «*1. Il titolare del trattamento, tenuto conto delle cognizioni tecniche disponibili e dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate, quale la pseudonimizzazione, per garantire la protezione dei dati e per tutelare i diritti degli interessati, in conformità alle norme del presente decreto*».

[61] Reg. (UE) (UE) 2016/679 GDPR, art. 25: «*2. Tenendo conto dello stato dell'arte e dei costi di attuazione nonché della natura dell'ambito di applicazione del contesto e delle finalità del trattamento come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate […]*».

[62] D. lgs. 51/2018 art. 16: «*2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*».

[63] Reg. (UE) UE 2016/679 GDPR, art. 35: «*1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*».

In questo contesto si distingue la **probabilità**, ossia la stima calcolata a priori che accada un evento, dalla **frequenza**, che è il computo considerato a posteriori degli eventi accaduti.

A3.1.3 CALCOLO DEL RISCHIO

Il rischio è espresso comunemente e semplicemente con la formula:

$$R=P*M$$

ovvero

$$R=f(P,M)$$

R (risk) = **rischio**, definito come si è detto sopra;

P (hazard) = **pericolo**, ossia la probabilità o frequenza che si verifichi l'evento dannoso, ad esempio l'accesso non autorizzato all'archivio dei dati personali;

M (harm) = **magnitudo**, ossia la quantificazione del danno al verificarsi dell'evento in termini di soggetti coinvolti e di gravità, ad esempio la quantità di dati personali e il numero di soggetti coinvolti.

Questo modello è quello utilizzato anche dalle Linee guida DPIA, che definisce il rischio in funzione proprio di pericolo e magnitudo (cap. III par. 2 Linee Guida DPIA).

A3.1.4 LA VALUTAZIONE PRELIMINARE DEL RISCHIO

La normativa in materia e le indicazioni del WP29 (Article 29 Working Party o WP29, previsto dall'art. 29 della direttiva europea 95/46) non indicano un modello specifico da adottare, tuttavia sono disponibili, con valore indicativo e senza alcun vincolo o valore normativo, i framework di DPIA realizzati dalle diverse autorità nazionali di controllo.

- Framework CNIL - Commission Nationale de l'Informatique et des Libertés https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia;
- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf;
- Agencia española de protección de datos https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf;
- Information Commissioner's Office https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

Questi sistemi tuttavia non sono assolutamente esaustivi e non hanno nemmeno la pretesa, mai asserita, di assolvere al compito del complesso processo di valutazione d'impatto-DPIA che è rimesso al tecnico esperto e competente scelto dal titolare del trattamento secondo il principio dell'accountability (art. 35 par. 1 GDPR, art. 23 c. 1 d. lgs. 51/2018) di cui si è detto in precedenza.

Lo scopo di questi framework, elaborati anni orsono e oggi sicuramente da valutare nella loro attualità, è quello di offrire al titolare una percezione di massima del rischio del trattamento al fine di valutare l'opportunità di svolgere la valutazione d'impatto-DPIA che dovrà fare riferimento alle norme internazionali di standardizzazione ISO per essere in grado di dimostrare concretamente il rispetto effettivo della normativa europea sulla protezione dei dati, che è il senso dell'accountability e la sua definizione normativa.

A3.1.5 LA GESTIONE DEL RISCHIO SECONDO LA NORMA ISO

La ISO ha pubblicato una linea guida per effettuare un DPIA (ISO/IEC 29134), definendo un processo per la privacy impact assessment con una struttura e i relativi contenuti del report della valutazione d'impatto sulla protezione dei dati-DPIA a supporto del principio di accountability.

Il rischio è identificato, misurato secondo la normativa internazionale dello standard ISO (International Organization for Standardization) 31000 su "*Gestione del rischio – Principi e linee guida*", definisce il rischio come "*effetto dell'incertezza sugli obiettivi*"[64], che definisce:

- **effetto** è lo scostamento rispetto al risultato atteso, sia in senso positivo che negativo;
- **obiettivi** possono coprire diversi settori, come ad esempio i dati personali trattati, e possono essere applicati a diversi livelli: il livello strategico, il livello organizzativo, l'ambito della produzione e dell'operatività;
- **rischio** è solitamente caratterizzato dall'accadimento di eventi e di conseguenze di questi eventi, ed è valutato in termini di valore delle conseguenze di un determinato accadimento e probabilità di occorrenza dell'evento;
- **incertezza** costituisce la componente non conosciuta associata alla probabilità dell'evento e alle conseguenze che ne derivano nella pratica.

L'effetto di cui parla la definizione dell'UNI EN ISO 31000 è semplicemente un risultato diverso da quello atteso e può essere sia negativo che positivo e può in seguito creare in cascata successive opportunità e minacce.

Il rischio è espresso dalle fonti di rischio, che sono gli elementi da cui può originare, e dagli eventi causali, che sono i fatti che possono concretizzare l'effetto potenziale della fonte di rischio.

A3.1.6 IL PROCESSO DI VALUTAZIONE DEL RISCHIO

Il processo risk evaluation e risk management secondo lo standard ISO, si basa sul ciclo di Deming[65] o ciclo PDCA (Plan/Do/Check/Act), un sistema di gestione iterativo in quattro fasi utilizzato per il controllo e il miglioramento continuo dei processi che consiste in quattro fasi:

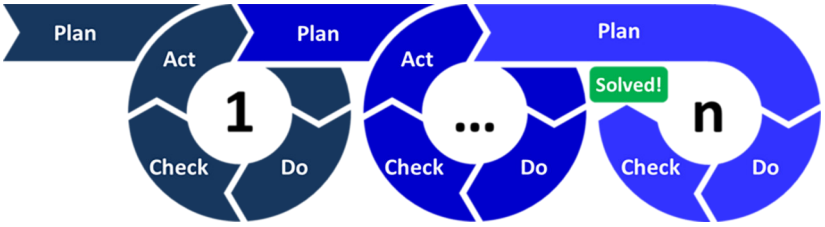
- **Plan**, stabilire gli obiettivi e i processi necessari per fornire risultati in accordo con i risultati attesi ossia cosa fare e come farlo (pianificazione) per soddisfare politica e obiettivi che si sono determinati;
- **Do**, esecuzione di quanto pianificato, dapprima in contesti circoscritti;

---

[64] ISO (International Organization for Standardization) 31000:2010, 2 (Termini e definizioni) 2.1: «*rischio: Effetto dell'incertezza sugli obiettivi. Nota 1 Un effetto è uno scostamento da quanto atteso - positivo e/o negativo. Nota 2 Gli obiettivi possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione). Nota 3 Il rischio è spesso caratterizzato dal riferimento a eventi (2.17) potenziali e conseguenze (2.18), o una combinazione di questi. Nota 4 Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della verosimiglianza (2.19) del suo verificarsi. Nota 5 L'incertezza è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro verosimiglianza.*».

[65] William Edwards Deming (1900-1993) è stato un ingegnere, saggista, docente e consulente di gestione aziendale e manager statunitense. A Deming fu ampiamente riconosciuto il merito per gli studi sul miglioramento della produzione negli Stati Uniti d'America durante la seconda guerra mondiale, anche se egli è forse più noto per il suo lavoro in Giappone (Ciclo di Deming).

- **Check**, verificare se si è fatto quanto pianificato e se quanto fatto risulta efficace al raggiungimento degli obiettivi, studiando e raccogliendo i dati sui risultati per verificarne le eventuali differenze.
- **Act**, le azioni per rendere definitivo o migliorare il processo, estendendo quanto testato dapprima in contesti circoscritti all'intera organizzazione, attuare azioni correttive sulle differenze significative tra i risultati effettivi e previsti, analizzando le differenze per determinarne le cause e dove applicare le modifiche per migliorare il processo.



A3.1.7 METODO DI VALUTAZIONE

Il metodo di valutazione di risk management secondo la norma ISO 31000 si compone di quattro fasi che si ripetono in modo circolare:

1. **individuazione del rischio;**
2. **quantificazione del rischio;**
3. **valutazione del rischio;**
4. **controllo del rischio.**

Nel dettaglio ciò comporta:

1. Individuazione del rischio

La prima fase è l'individuazione e la catalogazione dei rischi per area di rischio, aggiungendo a ognuno una descrizione qualitativa. L'individuazione dei rischi può essere fatta sull'intero processo dai trattamenti al Comune di Santeramo in Colle ovvero su un singolo processo, in base alle necessità evidenziate dal titolare del trattamento esplicitate nell'affidamento di incarico come da determinazione del responsabile della Polizia Locale n. 1456/RG del 29/07/2026.

Quindi in questo caso si valuteranno esclusivamente i rischi connessi ai trattamenti eseguiti attraverso i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale.

Per l'individuazione del rischio in questa fase devono essere acquisiti tutti i dati e la documentazione necessaria e devono partecipare tutte le persone coinvolte nel trattamento e in particolare:

- il sindaco del Comune di Santeramo in Colle nel suo ruolo di legale rappresentante del titolare del trattamento;
- i dirigenti, i funzionari di elevata qualificazione (EQ) e il segretario generale, nei casi in cui non svolga esclusivamente le funzioni di cui all'art. 97 c. 4 TUEL ovvero il direttore generale, qualora sia stato nominato (art. 108 TUEL), nei casi in cui non si limiti a coordinare e sovrintendere allo svolgimento delle funzioni dei dirigenti ma disponga anche di propria autonomia gestionale in ordine ai trattamenti dei dati personali;
- eventuali contitolari del trattamento (art. 26 GDPR e art.17 d. lgs. 51/2018), che in questo caso non ci sono;

- eventuali responsabili del trattamento (art. 4 par. 1 p. 7 GDPR e art. 18 d. lgs. 51/2018), attualmente: Gestione Servizi s.p.a..

2. Quantificazione del rischio

La fase di quantificazione del rischio si occupa di valutare i singoli rischi, uno ad uno per quanto riguarda la probabilità che si concretizzino ossia secondo il test del **rapporto di verosimiglianza (LR)** o *likelihood ratio test* come si indica nel contesto internazionale ISO del risk management, oltre che le potenziali conseguenze di questa concretizzazione.

Una volta valutati i rischi singolarmente sarà necessario valutare quali conseguenze possono avere nel corso del tempo i rischi correlati tra loro o sovrapposti procedendo quindi all'analisi dell'aggregazione del rischio).

Gli **indicatori chiave del rischio** o *Key Risk Indicators* (acronimo KRI) sono componenti del processo di valutazione e quantificazione nell'ambito del risk evaluation e risk management e sono utilizzati per fornire indicatori di guida o di marcatura per le potenziali condizioni di rischio.

Ogni istanza di un KRI all'interno dell'organizzazione può avere dei limiti di destinazione e di soglia unici e i valori KRI sono utilizzati per registrare il valore effettivo di un indicatore in un momento specifico.

I metodi di quantificazione del rischio dipendono dal contesto ambientale e dalla tipologia dell'ente coinvolto, in base ai KRI che sono stati definiti preventivamente.

3. Valutazione del rischio

La valutazione del rischio si compone di tutte le attività e le iniziative che il Comune di Santeramo in Colle può mettere in campo per rispondere a tutti i rischi individuati.

L'elenco di queste misure è fatto nel dettaglio e può riguardare sia misure specifiche per rischi specifici che misure generiche adattabili a vari rischi.

Le iniziative per ridurre il rischio si possono dividere in:

- **reazioni attive preventive**, che riducono la possibilità che si verifichi un rischio agendo sulle cause di esso, ad esempio migliorando una procedura, riducendo i rischi di responsabilità;
- **reazioni passive correttive**, che trasferiscono a un altro soggetto le conseguenze dell'insorgenza del rischio, ad esempio sottoscrivendo un'assicurazione.

Anche dopo tutte le misure che il titolare del trattamento mette in campo per evitare le conseguenze del rischio rimane comunque un rischio residuale, ovvero la possibilità che il Comune di Santeramo in Colle subisca le conseguenze di un rischio si avveri nonostante le misure di controllo e prevenzione adottate.

4. Controllo del rischio

In quest'ambito si verificano l'efficienza e l'efficacia dei metodi applicati per la gestione del rischio, che sono diversi in base al tipo di rischio e alla tipologia di ente/servizio/progetto.

A3.1.8 IL MODELLO A TRE LINEE DI DIFESA-THREE LINES OF DEFENSE (3LOD)

1. Definizione

Il processo di gestione dei rischi non può e non deve essere interamente responsabilità di una singola persona, ma deve diventare un obiettivo condiviso da tutti i soggetti coinvolti nel trattamento.

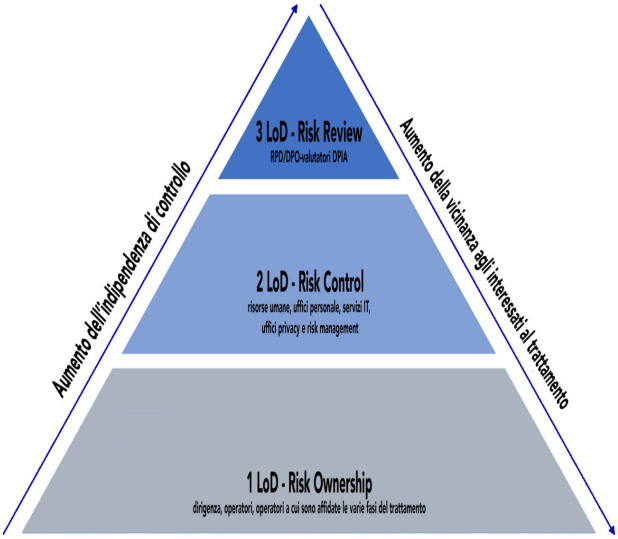
L'Institute of Internal Auditors[66] ha elaborato un modello definito "*The IIA's Three Lines of Defense Model*", traducibile in **Modello a tre line di difesa**, che in precedenza era noto come "*The Three Lines of Control for Effective Risk Management and Control*", che propone un approccio che integra i livelli di governance nella gestione e controllo dei rischi.

Il modello si applica a tutte le organizzazioni, a prescindere dalla natura pubblica o privata, dalle dimensioni, dal settore, in quanto i principi in cui si sviluppa sono implementabili in qualsiasi tipo di realtà e sono:

a. **forte governance**, intesa soprattutto come accountability;

b. **definizione delle procedure**, in particolare di processi e strutture adeguate per il raggiungimento degli obiettivi, in particolare di quelle per la mitigazione del rischio e di sorveglianza e aggiornamento sui rischi del trattamento;

c. **separazione e controllo reciproco** tra la prima linea della governance, costituita dai vertici decisionali ossia i responsabili degli uffici del Comune di Santeramo in Colle, e la seconda linea della operatività, costituita dagli operatori che svolgono il trattamento, che si controllano e verificano ordinariamente e costantemente per garantire il rispetto delle norme (compliance), gestendo i rischi con comportamenti etici;



d. **presenza di una terza linea di audit** che assicuri in modo obiettivo e indipendente l'adeguatezza e l'efficacia della governance e dei processi di gestione del rischio;

e. **indipendenza della terza linea**, per garantire l'obiettività di assurance e advice;

f. **sinergia di tutti i ruoli** per creare e proteggere valore e garantire efficacia e legalità dell'azione dell'ente, in allineamento tra di loro e con le priorità fissate dei vari stakeholders, ossia dai ruoli di indirizzo politico e di direzione amministrativa.

2. Struttura

Questo modello permette di istituire un sistema in cui tre separati livelli dell'ente agiscono controllando il rischio e supervisionandosi tra loro, in modo da riuscire a prevenire, per quanto possibile, l'errore umano:

- **Prima linea di difesa (1LoD)-Risk Ownership**: si occupa della definizione dei trattamenti e delle procedure operative per attuarli, devono inserire la gestione del rischio nel proprio processo decisionale e assicurarsi che la seconda linea agisca in modo conforme al processo di risk management, si occupano anche dell'attuazione dei trattamenti e quindi sono il livello più vicino agli interessati (DS) al trattamento.

[66] L'Institute of Internal Auditors [Istituto dei revisori interni] è un'associazione professionale internazionale fondata nel 1941 che offre conferenze educative e sviluppa standard, linee guida e certificazioni per l'internal audit. Ha sede a Lake Mary, Florida, negli Stati Uniti. https://www.theiia.org.

Soggetti coinvolti: i 1responsabili degli uffici del Comune di Santeramo in Colle e il segretario generale, nei casi in cui non svolga esclusivamente le funzioni di cui all'art. 97 c. 4 TUEL ovvero il direttore generale, qualora sia stato nominato (art. 108 TUEL) e non si limiti a coordinare e sovrintendere allo svolgimento delle funzioni dei dirigenti ma disponga anche di propria autonomia gestionale in ordine ai trattamenti dei dati personali, e tutti gli operatori a cui sono affidate le varie fasi del trattamento.

- **Seconda linea di difesa (2LoD)-Risk Control**: supporta i process owner, offrendo le proprie specifiche competenze per verificare la corretta attuazione delle privacy policies e l'adeguatezza delle stesse allo scenario operativo.

  Soggetti coinvolti: risorse umane, uffici personale, servizi IT, uffici privacy e risk management che devono svolgerle tenendo presente le logiche di risk management, assicurandosi che la prima linea prenda decisioni coerenti con esse.

- **Terza linea di difesa (3LoD)-Risk Review**: svolge verifiche indipendenti e oggettive sull'attività della prima e seconda linea, per rilevare i rischi e accertare la conformità della gestione alle norme tecniche e giuridiche sul trattamento dei dati personali.

  Soggetti coinvolti: il RPD/DPO e l'ente certificatore che ha redatto la presente valutazione d'impatto, i quali, rispettivamente, vigilando costantemente e verificando periodicamente l'operato della prima e seconda linea controllano che il processo di risk management sia attuato correttamente dalle parti.

Sezione A4 -Metodologia operativa di svolgimento della valutazione

A4.1 Premessa metodologica

A4.1.1 PROCEDURA OPERATIVA E FASI SPECIFICHE

Il processo complessivo di misurazione del rischio assegna un giudizio per ogni sezione della valutazione, analizzando attentamente i rischi e quindi quantificandoli secondo parametri omogenei e predefiniti, avendo sempre come principio quello dell'accountability (art. 35 par. 1 GDPR e art. 23 c. 1 d. lgs. 51/2018).

La valutazione d'impatto-DPIA (Data Privacy Impact Assessment) quindi è un processo codificato e strutturato in fasi, uno strumento operativo che consente di analizzare con sistematicità e periodicamente il trattamento per individuare e a ridurre i rischi privacy per gli individui interessati coinvolti dal rilascio di un nuovo progetto, soluzione o regola costituisce parte integrante dell'approccio privacy by design, ed aiuta ad assicurare che i problemi potenziali siano identificati negli stadi iniziali del progetto quando la possibilità di indirizzarli è spesso più efficace e meno costosa.

Le sue fasi devono avere un ciclo ricorsivo per attualizzare la valutazione fatta inizialmente a mano a mano che si procede con il progetto e vengono attuate le misure pianificate.

Le fasi del processo DPIA possono essere condotte e registrate secondo il seguente schema:

1. **valutazione preliminare della necessità e opportunità;**
2. **descrizione dei flussi di informazioni e coinvolgimento dei partecipanti;**
3. **identificazione dei rischi nel trattamento dei dati;**
4. **pianificazione della riduzione del rischio;**
5. **approvazione delle decisioni e registrazione dei risultati;**

6. **integrazione dei risultati della DPIA e dei documenti collegati.**

Nel dettaglio ciò comporta:

a) Valutazione preliminare della necessità e opportunità

Questa fase serve in generale a:

- spiegare ciò che il progetto intende realizzare;
- esprimere i benefici attesi per l'organizzazione;
- decidere per gli individui e le altre parti, in base ad un insieme di domande mirate di screening, se la DPIA sia necessaria per dimensionare le risorse a seconda dell'entità del progetto e il tempo necessario alla valutazione capire gli impatti potenziali e i passi che potrebbero essere richiesti per identificare e ridurre il rischio.

Nel caso di specie la valutazione è riferita ai sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale e quindi rientra nei casi obbligatori di svolgimento della DPIA (art. 35 GDPR e Linee guida videosorveglianza), pertanto sussistendo la necessità non si procede ad alcune valutazione di opportunità.

b) Descrizione dei flussi di informazioni e coinvolgimento dei partecipanti

In questa fase si esegue una valutazione approfondita dei rischi e delle conseguenze per la sicurezza dei dati personali degli interessati valutando approfonditamente gli elementi che caratterizzano il trattamento dei dati descrivendo:

- quali informazioni sono utilizzate;
- come vengono trattate nelle singole fasi;
- a cosa servono, ovvero per quale finalità;
- da chi sono ottenute, a chi sono comunicate;
- chi ne deve avere accesso.

Il processo di definizione della DPIA può essere supportato da fonti informative già disponibili all'interno dell'organizzazione per descrivere come i dati saranno utilizzati, ad es. un diagramma che riporti i flussi informativi tra i vari soggetti o sistemi, la sequenza prevista delle operazioni di gestione dei dati, rapporti di audit, mappe informative, registri di assets informativi.

In questa fase svolgono un ruolo fondamentale tutti i soggetti che partecipano a vario titolo al trattamento, compresi eventuali contitolari e responsabili dei trattamenti.

Essi guidano la fase di ricostruzione dei flussi dei dati e degli stadi di processo (ad es. acquisizione presso terzi ovvero raccolta dall'interessato, data entry, archiviazione strutturata, estrapolazione dei dati, trasmissione a eventuali responsabili del trattamento, ecc.) evidenziando le possibili criticità e rischi, illustrando eventuali precedenti valutazioni d'impatto e descrivendo le nuove procedure.

c) Identificazione dei rischi nel trattamento dei dati

In questa fase si analizza l'intero processo di trattamento per identificare e valutare le fasi che possono presentare rischi per la sicurezza dei dati in un'ottica di risk assessment e di risk management secondo le norme internazionali di standardizzazione indicate in precedenza[67].

[67] Vds. il paragrafo *A3.1.5 la gestione del rischio secondo la norma ISO* a pag. 22.

L'identificazione dei rischi si basa sulla descrizione dei flussi informativi svolta nella fase precedente, raggruppando gli stadi di utilizzo dei dati come una sequenza logica dei trattamenti, da quando i dati vengono ricevuti dall'esterno a quando vengono aggregati, elaborati, storicizzati e poi ulteriormente trasferiti.

È importante applicare a questi stadi dei dati un set di quesiti che consenta di far emergere le vulnerabilità e le minacce e su queste determinare gli effetti su cui quantificare gli impatti.

Laddove esistenti si possono utilizzare standard di settore o propri e metodologie di project management o di risk management per aiutarsi a categorizzare, identificare e misurare i rischi.

Il rischio deve essere valutato in termini di coefficienti di probabilità e di gravità secondo scale numeriche associate a classi di valori di cui si è già illustrato in precedenza[68].

d) Pianificazione della riduzione del rischio

Dopo aver dettagliatamente individuato e misurato i rischi nella fase precedente, si procede a elaborare un piano di attenuazione del rischio cercando soluzioni che siano adeguatamente efficaci e sufficientemente rapide tra le varie opzioni disponibili.

Lo scopo della pianificazione non è quello di eliminare completamente l'impatto, poiché non è possibile avere assenza di qualsiasi rischio, ma è quello di ridurre la frequenza e la magnitudo di ogni rischio a un livello accettabile che, comunque, consenta di realizzare il trattamento valutato.

In questa fase è opportuno documentare la misura di riduzione di rischio che ogni soluzione intende apportare e quantificare i costi e i benefici delle possibili soluzioni. Alcuni costi possono essere di natura prettamente finanziari, ad esempio quando deve essere acquistato un nuovo software per garantire un maggiore controllo sull'accesso e sulla conservazione, ma i maggiori costi devono essere bilanciati rispetto ai benefici attesi, come per esempio una maggiore garanzia per proteggersi da violazioni dei dati, un minore rischio di sanzioni o provvedimenti o di essere esposti a effetti reputazionali.

e) Approvazione delle decisioni e registrazione dei risultati

Nell'ottica dell'accountability si deve tenere traccia e argomentare il percorso decisionale che ha portato alla scelta delle misure e delle tempistiche dell'eventuale piano di riduzione del rischio ovvero della scelta di accettare i rischi emersi dalla presente valutazione e deve essere esplicita l'argomentazione sostenuta e l'assunzione di responsabilità.

La relazione finale del team di valutatori che hanno redatto il presente atto, il parere del responsabile per la protezione dei dati RPD-DPO, le decisioni del titolare del trattamento che sono parti integranti e motivazione dell'atto di approvazione del presente documento, consentono a posteriori di argomentare le scelte fatte sulla base dei rischi individuati, secondo il metodo dell'accountability che obbliga il titolare a dimostrare la conformità al GDPR.

f) Integrazione dei risultati della DPIA e dei documenti collegati

Il presente documento, all'atto dell'approvazione, integra i seguenti atti:

- misurazione del rischio elaborata dal team dei valutatori, decisione del titolare del trattamento ed eventuali rilievi e segnalazioni formulati dai soggetti interessati o coinvolti;
- parere del DPO, se richiesto dal titolare (art. 39 par. 1 lett. c GDPR).

[68] Vds. la sezione *A1.7 Il metodo standardizzato per la valutazione e gestione del rischio* a pag. 11.

Le revisioni successive e gli aggiornamenti devono integrare o comunque indicare ove reperire la precedente valutazione d'impatto-DPIA e compararne i risultati nelle parti in cui fossero emersi nuovi rischi o si fossero aggravati o mitigati quelli già evidenziati e valutati.

Il rischio non si esaurisce mai ma può evolversi, quindi le revisioni possono allungarsi o abbreviarsi ma non si può mai ritenere che la valutazione d'impatto sulla protezione dei dati costituisca un punto di arrivo definitivo e non la si potrà mai considerare un documento statico e immutabile.

A4.2 Algoritmo di valutazione

A4.2.1 ALGORITMO DI VALUTAZIONE DEL RISCHIO INIZIALE O EMERGENTE

Il processo di valutazione seguito, in conformità alla metodologia indicata in precedenza, assegna un punteggio per ogni sezione analizzata secondo il rischio che si osserva inizialmente, detto con terminologia anglosassone standardizzata "*as is*", e che quindi emerge e precisamente per:

- **Sezione B1-Descrizione generale del trattamento;**
- **Sezione B2-Valutazione della necessità e proporzionalità;**
- **Sezione B3-Valutazione del rischio sui diritti e le libertà degli interessati;**
- **Sezione B4-Valutazione degli strumenti del progetto operativo;**
- **Sezione B5-Valutazione del posizionamento dei sistemi di ripresa.**

Sulla base delle criticità rilevate si misurerà il rischio emergente al momento della valutazione, assegnando per ogni sezione un duplice punteggio sulla base dei valori di:

a. **Magnitudo emergente (Me)**, ossia il valore stimato della gravità emergente delle conseguenze dell'evento qualora si verificasse, secondo matrice che segue:

Valore	Entità delle conseguenze (Me)	Descrizione degli eventi
1	Trascurabili	nessuno di rilievo
2	Marginali	gli interessati non incontrano inconvenienti significativi
3	Limitate	gli interessati possono incontrare significativi disagi che potranno superare nonostante alcune difficoltà (*ad es. costi aggiuntivi, problemi nell'accesso ai servizi, paura, stress, disturbi fisici minori*).
4	Gravi	gli interessati possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà (*ad es. danni economici, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute*).
5	Gravissime	gli interessati possono avere conseguenze significative irreversibili, che non possono superare (*ad es. incapacità lavorativa, disturbi psicologici o fisici, morte*).

b. **Pericolo emergente (pe)**, ossia il valore stimato della probabilità o frequenza, valutata al momento dell'osservazione, che si verifichi l'evento dannoso secondo la seguente matrice:

Valore	Probabilità dell'evento (pe)	Probabilità stimata che l'evento accada nell'anno
1	Raro	< 5%
2	Poco probabile	>5% < 20%

3	Probabile	>20% < 50%
4	Molto probabile	>50% < 70%
5	Estremamente probabile	> 70%

A4.2.2 RISCHIO EMERGENTE (RE)

Il rischio emergente è dato dal prodotto: **Re=p*M** giudicato secondo la seguente matrice:

		RISCHIO EMERGENTE (Re)				
PROBABILITÀ (p)	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		CONSEGUENZE (M)				

VALORE	DEFINIZIONE DEL RISCHIO EMERGENTE (Re)
Re<=4	Basso
4<Re<=8	Medio
8<Re<=12	Rilevante
Re>12	Alto

A4.2.3 ALGORITMO DI VALUTAZIONE PARTICOLARE PER OGNI SEZIONE

Ogni sezione valuta 10 rischi, tranne l'ultima che ne considera 9, per ogni rischio è attribuito un valore da 0 a 2 per la magnitudo (M) che valuta le conseguenze attese secondo i seguenti valori:

VALORE	CONSEGUENZE ATTESE (M)
0	Trascurabili
0,5	Marginali
1	Rilevanti
1,5	Gravi
2	Molto gravi

Inoltre è attribuito un valore da 0 a 1 per il pericolo (p) che l'evento accada:

VALORE	FREQUENZA ATTESA (M)	% probabilità
0	Raro	<5%
0,25	Poco probabile	5%-20%

0,5	Probabile	20%-50%
0,75	Molto probabile	50%-70%
1	Estremamente probabile	>70%

A4.3 Esiti finali della DPIA

A4.3.1 Conseguenze della valutazione finale

Acclarato che l'obiettivo sostanziale della DPIA è quello di rendere più vicino possibile allo zero il rischio di procurare danni alle libertà e ai diritti o all'interessato, essa compie una valutazione puntuale dello stato di fatto ("*as is*") ponendo la sua attenzione sui rischi legati al trattamento e valutandoli al netto delle attività poste in essere o Pianificate per contenerlo e ridimensionarlo sulla base delle valutazioni del titolare del trattamento e del suo staff.

All'esito dello svolgimento della valutazione d'impatto il rischio residuo, che non può mai essere nullo per definizione, si può gestire in differenti modalità:

a. **prevenzione del rischio**, la prevenzione è un metodo per mitigare i rischi che prevede la rinuncia a compiere azioni compromettenti per l'organizzazione;
b. **riduzione del rischio**, questo metodo di gestione del rischio ha come obiettivo quello di minimizzare le perdite pur accettando il rischio e quindi ci si concentra sul contenimento e sulla prevenzione della sua diffusione;
c. **condivisione del rischio**, ottenuto trasferendo il rischio da un singolo o da un gruppo a un gruppo più ampio;
d. **trasferimento del rischio** a terze parti che possano gestire o assicurare l'evento e/o le conseguenze;
e. **accettazione e conservazione del rischio**, come forma residuale di tutte le altre misure poiché tutte le misure di condivisione, trasferimento e riduzione del rischio, non eliminano mai del tutto il rischio residuo.

A4.3.2 Gestione dei rischi

La gestione del rischio è un sistema di persone, processi e tecnologie che consente a un'organizzazione di stabilire obiettivi in linea con valori e rischi.

Perché un programma di valutazione del rischio sia efficace, deve soddisfare obiettivi legali, contrattuali, interni, sociali, etici e a monitorare le nuove normative in materia di tecnologia concentrando l'attenzione sul rischio e impegnando le risorse necessarie per controllarlo e mitigarlo.

Nel processo di gestione del rischio le fasi importanti sono:

- **identificazione del rischio**;
- **analisi e valutazione del rischio**;
- **mitigazione e monitoraggio del rischio**.

Gli standard di gestione del rischio definiscono un insieme specifico di processi strategici finalizzzati a individuare i rischi e promuoverne la mitigazione attraverso le best practices e gli standard internazionali definiti oggettivamente, come lo standard ISO 31000 sulla gestione del rischio che fornisce principi e linee guida per una gestione efficace del rischio.

Nei casi in cui il rischio si presentasse più grave che non accettabile, si prevederanno e attueranno misure di riduzione e compensazione delle criticità e in questo caso si procederà a rivalutare il rischio.

Qualora il titolare riesca con il processo di DPIA a identificare correttamente e a eliminare o attenuare sufficientemente il rischio, inizia il trattamento dopo aver completato la valutazione d'impatto, con il percorso previsto dal GDPR, rendendo disponibile la DPIA agli organi di controllo e a chi ne abbia titolo.

Viceversa, ma anche contestualmente, si applica un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando così un indice di rischio "normalizzato" rispetto al contesto ove avviene il trattamento valutato nel presente documento.

La presente valutazione terrà conto solo del rischio assoluto, nelle successive, applicando il ciclo di Deaming illustrato in precedenza, valuterà negli esiti finali il rischio normalizzato verificando sul campo l'efficacia delle misure di mitigazione del rischio.

A4.3.3 RISCHIO RESIDUO (RR)

Il processo di gestione del rischio deve essere valutato nei suoi effetti sul **rischio emergente** (**Re**) calcolando il **rischio residuo** (**Rr**) che tiene conto del fattore **vulnerabilità** (**Vu**) del sistema in funzione del grado di adeguatezza delle misure di sicurezza, valutato in tre condizioni secondo la seguente matrice:

VALORE	ADEGUATEZZA DELLE MISURE (Vu)
0,25	Adeguate
0,5	Parzialmente adeguate
1	Inadeguate

Il rischio residuo (Rr) è dato quindi dal prodotto del rischio emergente per la vulnerabilità, secondo la formula: **Rr=Re*Vu e** giudicato con la seguente matrice:

		VALORE DEL RISCHIO RESIDUO (Rr)					
Vu	1	Rr=4	4<Rr<=6	6<Rr<=8	8<Rr<=9	9<Rr<=12	Rr>12
	0,5	Rr<=2	2<Rr<=3	3<Rr<=4	4<Rr<=6		6>Rr>9
	0,25	Rr<=1	1<Rr<=2		2<Rr<=3		3<Rr>6
		Re<=4	4<Re<=8		8<Re<=12		Re>12
		RISCHIO EMERGENTE (Re)					

Il valore del rischio residuo è giudicato su quattro valori secondo la seguente tabella:

VALORE	RISCHIO RESIDUO (Rr)
Rr<=3	Molto basso
3<Rr<=6	Basso
6<Rr<=9	Rilevante
Rr>9	Alto

A4.3.4 SUSSISTENZA RESIDUA DI RISCHI ELEVATI E PROCEDURA DI PARERE PREVENTIVO

Quando all'esito della valutazione d'impatto si ritenga che sussistano rischi elevati anche dopo l'applicazione delle misure di sicurezza, il trattamento non può aver luogo e si deve procedere alla preventiva consultazione del Garante (art. 36 GDPR[69]), e ciò vale anche per i trattamenti esclusi dal GDPR (art. 24 c. 1 d. lgs. 51/2018[70]) in questo caso il titolare o il responsabile del trattamento devono inviare la DPIA[71] all'Autorità di controllo comunicando:

a) **le finalità e i mezzi del trattamento** (art.36 p. 3 lett. b GDPR[72]);
b) **i ruoli deputati al trattamento** dettagliando le responsabilità del titolare del trattamento, l'eventuale presenza e l'accordo con i contitolari del trattamento, la nomina di responsabili del trattamento, il tutto con particolare attenzione nel caso in cui il trattamento avvenga nell'ambito di un gruppo imprenditoriale (art.36 p. 3 lett. a GDPR[73]);
c) **le misure di sicurezza** che sono state previste per proteggere i diritti e le libertà degli interessati e per rendere quindi il trattamento conforme al regolamento (art.36 p. 3 lett. c GDPR[74]);

[69] Reg. (UE) 2016/679 GDPR, art.36 (Consultazione preventiva): «*1.Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.*».

[70] D. lgs. 51/2018 art. 24 (Consultazione preventiva del Garante): «*1. Salvo quanto previsto dall'articolo 37, comma 6, il titolare del trattamento o il responsabile del trattamento consultano il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se: a) una valutazione d'impatto sulla protezione dei dati di cui all'articolo 23 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure b) il tipo di trattamento presenta un rischio elevato per i diritti e le libertà degli interessati anche in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici.*».

[71] Reg. (UE) 2016/679 GDPR, art.36: «*3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;[...]*».

[72] Reg. (UE) 2016/679 GDPR, art.36: «*3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:[...] b) le finalità e i mezzi del trattamento previsto;[...]*».

[73] Reg. (UE) 2016/679 GDPR, art.36: «*3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;…*».

[74] Reg. (UE) 2016/679 GDPR, art.36: «*3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:[...] c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;[...]*».

d) **i dati e i recapiti del responsabile della protezione dei dati/data protection officer (RPD/DPO)** indicando più modalità di contatto per facilitare l'accesso degli interessati al trattamento (art.36 p. 3 lett. d GDPR[75]) e non limitandosi alla sola pec;

e) **ogni altra informazione utile** che sia richiesta dall'autorità di controllo (art.36 p. 3 lett. f GDPR[76] e art. 24 c. 4 d. lgs. 51/2018).

Ciò vale anche per i trattamenti dei dati personali finalizzati alla prevenzione, indagine, accertamento e perseguimento di reati e alla salvaguardia dell'ordine pubblico (art. 1 d. lgs. 51/2018), come avviene in questo caso da parte della Polizia Locale (art. 24 c. 1 d. lgs. 51/2018).

Il Garante fornisce un parere scritto entro otto settimane dalla richiesta di consultazione, il termine può essere ulteriormente prorogato di sei settimane nei casi di trattamenti particolarmente complessi, previo avviso (art. 36 p. 2 GDPR[77]) ovvero entro sei settimana, prorogabile di un ulteriore mese in casi eccezionali, per i soli trattamenti finalizzati alla prevenzione, indagine, acertamento e perseguimenti di reati e minacce all'ordine pubblico (art. 24 c. 5 e 6 d. lgs. 51/2018).

A4.3.5 ALTRI CASI IN CUI È RICHIESTA LA CONSULTAZIONE PREVENTIVA DEL GARANTE

A prescindere dalla sussistenza di rischi elevati anche dopo l'applicazione delle misure di sicurezza, l'invio della valutazione d'impatto-DPIA all'Autorità di controllo per il parere preventivo è sempre obbligatoria, a prescindere dal livello di rischio, nei casi tassativamente previsti nei quali il trattamento presenti:

- **un rischio elevato per i diritti e le libertà degli interessati** anche in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici (art. 35 p. 1 GDPR e art. 24 c. 1 lett. b d. lgs. 51/2018);
- **impiego di droni (aeromobili a pilotaggio remoto)** il cui impiego come strumento di videosorveglianza, consentito di norma solo per le forze di polizia, in considerazione della potenziale invasività è ricompreso sempre tra quelli che presentano rischi specifici (art. 23 c. 3 DPR 15/2018);
- **impiego di bodycam (telecamere indossabili)** il cui impiego è da considerarsi sempre ad alto rischio (GPDP provv. 291/2021[78]).

---

[75] Reg. (UE) 2016/679 GDPR, art.36: «*3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:[...] d) ove applicabile, i dati di contatto del responsabile della protezione dei dati;[...]*».

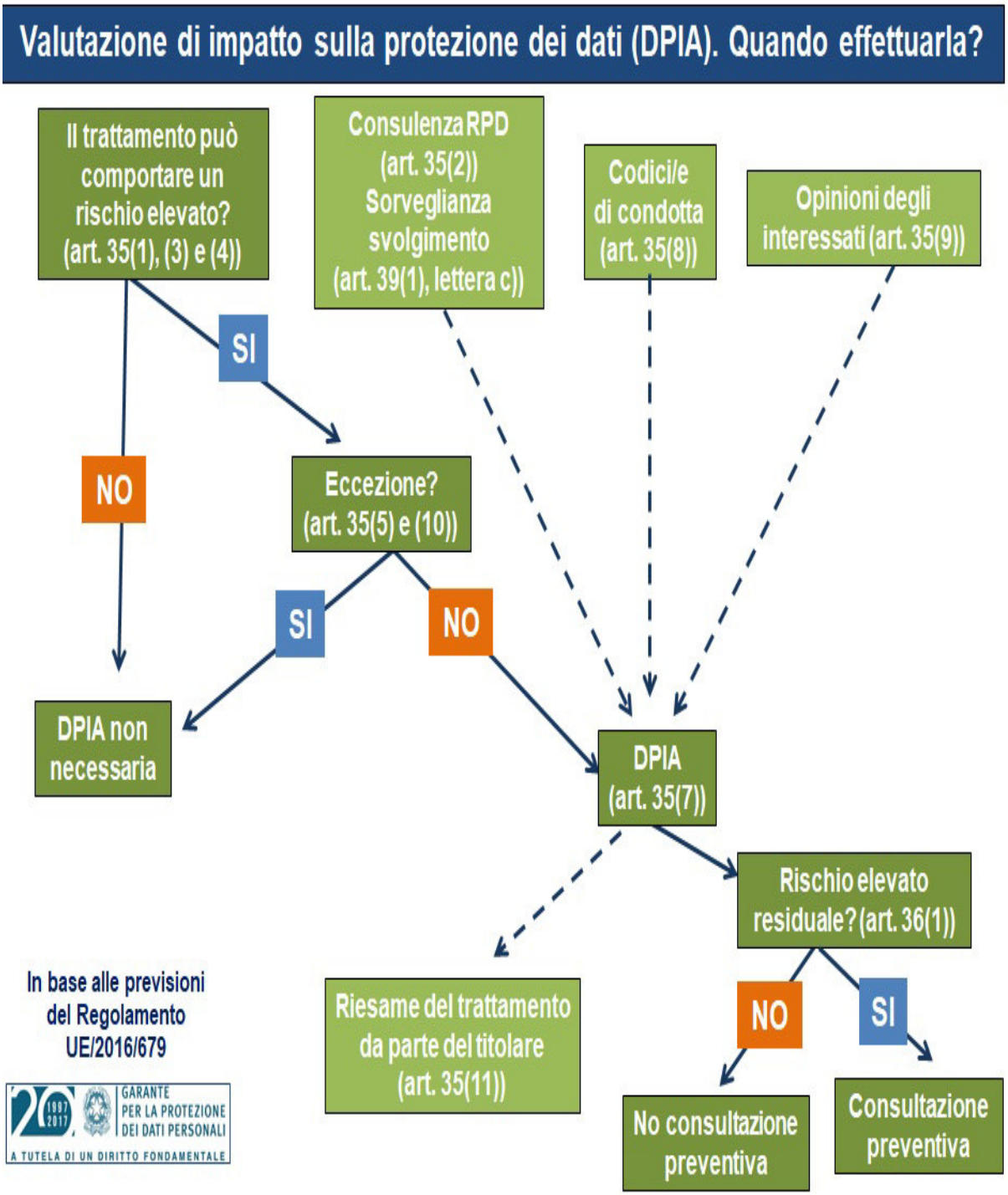
[76] Reg. (UE) 2016/679 GDPR, art.36: «*3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:[...] f) ogni altra informazione richiesta dall'autorità di controllo.*».

[77] Reg. (UE) 2016/679 GDPR, art.36: «*2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.*».

[78] Autorità Garante per la Protezione dei Dati Personali, provv. 291/2021 punto 4 pag. 7-8 *«[…omissis…] Pertanto, l'attività di trattamento in discussione va considerata a elevato rischio per gli interessati e, trovando applicazione l'articolo 24, par. 1, lett. a) del Decreto, si ritiene necessaria la consultazione preventiva.*».

A4.3.6 SCHEMA GRAFICO RIEPILOGATIVO DELLA PROCEDURA DPIA DISCIPLINATA DAL GDPR

Di seguito alcuni schemi grafici riepilogativi sull'obbligo di svolgere la valutazione d'impatto e sulle procedure di valutazione dello stesso e di svolgimento, ripresi dal sito del Garante per la protezione dei dati personali.



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** 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. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT.**

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

PARTE B-SVOLGIMENTO DELLA VALUTAZIONE D'IMPATTO

Lo svolgimento della presente valutazione d'impatto sulla protezione dei dati-data privacy impact assessment (DPIA) è relativa a i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale da parte del Comune di Santeramo in Colle.

Conformemente alle disposizioni della vigente normativa europea (art. 35 par. 7 GDPR[79] e Linee Guida EDPB 3/2019), si struttura come segue:

- **Sezione B1-Descrizione generale del trattamento previsto.**
- **Sezione B2-Valutazione della necessità e proporzionalità.**
- **Sezione B3-Valutazione dei rischi per i diritti e le libertà degli interessati.**
- **Sezione B4-Valutazione degli strumenti del progetto operativo.**
- **Sezione B5-Valutazione del posizionamento dei sistemi di ripresa.**
- **Sezione B6-Conclusioni, monitoraggio e revisione.**
- **Sezione B7-Documentazione allegata.**

Nella valutazione e quantificazione dei rischi relativi a ogni sezione si è seguito il seguente algoritmo:

a) **sono state enucleate delle aree omogenee di rischio**, numerate in maniera conseguenziale iniziando dal numero della sezione moltiplicato per 10, quindi per la sezione B1 si inizia dal numero 10, per la sezione B2 dal numero 20 e così via;

b) **per ogni area è stato attribuito un indice di magnitudo con valori compresi da 0 a 2** commisurato alle conseguenze qualora il rischio si verificasse (0=conseguenze trascurabili; 0,5=conseguenze marginali; 1=conseguenze rilevanti; 1,5=conseguenze gravi, 2,00=conseguenze molto gravi/gravissime);

c) **per ogni area è stato stimato un indice di pericolo con valori compresi valore da 0 a 1** commisurato alla probabilità che il rischio si verifichi (0=rara (<5%); 0,25=poco probabile (5%-20%); 0,5=probabile (20%-50%); 0,75=molto probabile (50%-70%); 1,00=estremamente probabile >70%);

d) **il valore finale è stato calcolato con prodotto tra la sommatoria della magnitudo e la sommatoria del pericolo, entrambe ricondotte al valore massimo di 5**, è stato attribuito a un range di 4 valori: basso (da 1 a 3); medio-basso (da 2 a 6); rilevante (da 8 a 12); alto (15-25).

[79] Reg. (UE) UE 2016/679 GDPR, art. 35: «*7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*».

Sezione B1-Descrizione generale del trattamento previsto

B1.1 Premessa

B1.1.1 OBBLIGO DI DESCRIZIONE GENERALE DEL TRATTAMENTO

La descrizione generale del trattamento complessivo è uno dei contenuti minimi della valutazione d'impatto-DPIA previsti dal GDPR (art. 35 par. 7 lett. a GDPR[80]) che richiede, tra l'altro, la descrizione sistematica del processo di trattamento dei dati personali estesa a tutti i trattamenti che presentino analogie per natura, ambito, finalità e rischi (art. 35 par. 1 GDPR[81]), svolti da un solo titolare o da più titolari (considerando 92[82]).

Anche nel caso di trattamenti svolti da organi, uffici e comandi di polizia, come sono quelli svolti dal titolare del trattamento attraverso la Polizia Locale di Santeramo in Colle, che sono esclusi dal campo di applicazione del GDPR e che sono finalizzati, in particolare, alla prevenzione, indagine, accertamento e perseguimento di reati e salvaguardia contro le minacce alla sicurezza pubblica (art. 1 c. 2 d. lgs. 51/2018), che nel caso di specie sono prevenzione, indagine, accertamento e perseguimento di reati, attività ausiliaria di salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 5 l. 65/1986 e art. 57 c.p.p.), con particolare riferimento alla sicurezza urbana (l. 48/2017), ed è espressamente previsto che la valutazione d'impatto-DPIA contenga, tra gli elementi fondamentali, la descrizione generale dei trattamenti (art. 23 c. 2 d. lgs. 51/2018[83]).

B1.1.2 ELEMENTI DESCRITTI IN QUESTA SEZIONE

Si procederà quindi a valutare:

1) **trattamento preso in considerazione;**
2) **soggetti di riferimento per il trattamento;**
3) **eventuali contitolari del trattamento;**
4) **responsabile per la protezione dei dati personali;**
5) **eventuali responsabili del trattamento;**
6) **eventuali trattamenti esternalizzati;**
7) **eventuale trasferimento in paesi terzi;**
8) **categorie d'interessati e tipologie di dati trattati;**
9) **eventuale parere degli interessati e standard applicabili;**

---

[80] Reg. (UE) 2016/679 GDPR, art.35: «*7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;[...]*».

[81] Reg. (UE) UE 2016/679 GDPR, art. 35: «*1. 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...*».

[82] Reg. (UE) UE 2016/679 GDPR, Considerando 92: «*Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata.*».

[83] D. lgs. 51/2018 art. 23: «*2. La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto.*».

10) [esattezza e aggiornamento dei dati e della valutazione](#)**.**

B1.2 Definizione e descrizione complessiva del contesto

B1.2.1 TRATTAMENTO PRESO IN CONSIDERAZIONE (RISCHIO §11)

La presente valutazione d'impatto-DPIA prende in considerazione il trattamento dei dati svolto dal Comune di Santeramo in Colle attraverso i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale, con l'impiego di 54 telecamere delle quali 50 di tipo fisso o comunque posizionate su installazioni inamovibili e 4 di tipo mobile o comunque non istallate in posizione fissa.

Il trattamento valutato nel presente atto non è organizzato da alcun atto e quindi è necessario provvedere al più presto ad adottare un disciplinare (art. 24 p. 1 GDPR) che preveda anche adeguate misure di sicurezza (art. 32 GDPR).

B1.2.2 SOGGETTI DI RIFERIMENTO PER IL TRATTAMENTO (RISCHIO §12)

I ruoli, le modalità e i mezzi del trattamento devono essere definiti dettagliatamente dal titolare del trattamento per espressa previsione di legge (art. 24 par. 1 GDPR e art. 15 d. lgs. 51/2018), le figure di riferimento che sono state comunicate dal titolare al momento sono indicate di seguito:

FUNZIONE	SOGGETTI
Titolare del trattamento-DC (art. 4 par. 1 n. 7 GDPR e art. 2 lett. h d. lgs 51/2018)	**Comune di Santeramo in Colle**, con sede in piazza Dottor Simone, 8 - 70029 Santeramo in Colle (BA), legale rappresentante avv. Vincenzo Luciano Casone nella sua qualità di sindaco, protocollo@pec.comune.santeramo.ba.it.
Responsabile protezione dati-RPD/DPO (art. 37-39 GDPR e art. 28-30 d. lgs 51/2018)	Giuseppe Nuzzolese, presso Municipio di Santeramo in Colle, piazza dottor Simone, 8 - Santeramo in Colle (BA), soggetto interno.
Soggetto designato per trattamenti di polizia esclusi dal GDPR (art. 2-quaterdecies Codice privacy, art. 19 d. lgs 51/2018 ai fini delle attività di cui art. 2 par. 2 lett. d GDPR e art. 1 c. 2 d. lgs. 51/2018)	comm. sup. dott. Vincenzo Caporusso, della Polizia Locale.
Contitolari del trattamento-JC (art. 26 GDPR e art. 17 d. lgs 51/2018)	nessuno.
Responsabili del trattamento-DP (art. 28 GDPR e, accidentalmente, ai fini art. 18 d. lgs. 51/2018)	Gestione Servizi s.p.a., sebbene in maniera irregolare.

I soggetti di riferimento per il trattamento sono definiti e nominati secondo i documenti che sono stati forniti, tuttavia la carenza di un disciplinare sul trattamento dei dati (art. 24 p. 1 GDPR) può costituire un pregiudizio nella definizione effettiva dei ruoli del trattamento e delle loro funzioni.

B1.2.3 EVENTUALI CONTITOLARI DEL TRATTAMENTO (RISCHIO §13)

Sono contitolari del trattamento, definiti anche *Joint Controllers* (JC), i distinti soggetti appartenenti a organizzazioni differenti e distinguibili che **stabiliscono congiuntamente le finalità e i mezzi del trattamento** (art. 26 GDPR e art. 17 c. 2 d. lgs. 51/2018), ossia il motivo e le modalità del trattamento e questo è l'elemento distintivo rispetto il soggetto che svolge una parte del trattamento per conto del titolare, quindi sotto la sua direzione e vigilanza, e per le finalità e con i mezzi da esso stabiliti, che assume viceversa il ruolo di responsabile del trattamento (art. 28 GDPR e art. 18 d. lgs. 51/2018).

La **partecipazione congiunta** può assumere la forma di **decisione comune**, quando è definita sin

dall'inizio da più soggetti, o delle **decisioni convergenti**, qualora decisioni autonome assunte dal titolari si integrino vicendevolmente e siano necessarie affinché il trattamento abbia luogo così da esplicare un effetto tangibile sulla definizione delle finalità e dei mezzi del trattamento (Linee guida titolare, pag. 3). L'esistenza di una responsabilità congiunta non implica necessariamente pari responsabilità dei vari operatori coinvolti nel trattamento dei dati personali che possono essere coinvolti in fasi e in misura diverse nel trattamento (Linee guida titolare p. 58, pag. 22).

Ciascun contitolare è tenuto a disporre di una base giuridica per il trattamento e a garantire che i dati non siano oggetto di ulteriore trattamento secondo modalità incompatibili con le finalità per le quali sono stati inizialmente raccolti da uno solo o da tutti i titolari, essi inoltre devono concordare e definire, con un atto certo e trasparente definito accordo di contitolarità ovvero joint controller agreement (JCA), le finalità, i mezzi del trattamento e le rispettive responsabilità per quanto concerne l'adempimento degli obblighi fissati dalla normativa in materia di protezione dei dati (considerando 79[84]).

Per essere qualificati come contitolari non è necessario che tale soggetto abbia accesso effettivo ai dati trattati, inoltre essi possono delegare ai responsabili del trattamento l'implementazione di aspetti pratici del trattamento ossia i c.d. "mezzi non essenziali" (Linee guida titolare, pag. 4).

Il titolare ha dichiarato che **non sono coinvolti altri soggetti come contitolari del trattamento (JC)**.

B1.2.4 RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RISCHIO §14)

Il responsabile della protezione dei dati personali (RPD), noto anche come *Data Protection Officer* (DPO), svolge un ruolo fondamentale nel trattamento dei dati e, nel caso degli enti pubblici com'è il titolare del trattamento valutato in questo atto, è una **figura necessaria e inderogabile** (art. 37 par. 1 lett. a GDPR[85]) anche nei trattamenti esclusi dal campo di applicazione del GDPR (art. 28 d. lgs. 51/2018[86]).

Questa figura ha la funzione di **fornire consulenza** al titolare o al responsabile del trattamento e ai dipendenti sugli obblighi derivanti dalla normativa sulla protezione dei dati personali e di **sorvegliare sull'osservanza**, fungendo da punto di contatto con l'autorità di controllo, se richiesto, fornisce il proprio parere sulla valutazione d'impatto sulla protezione dei dati e ne sorvegliarne lo svolgimento.

Non è richiesta alcuna abilitazione o titolo per svolgere il ruolo di RDO/DPO e la valutazione all'idoneità al ruolo è rimessa all'accountability del titolare del trattamento, ma sono prescritte come condizioni essenziali: l'indipendenza (art. 38 par. 3 lett. a GDPR[87]) nello svolgimento della funzione

---

[84] Reg. (UE) 2016/679 GDPR, considerando 79: «*La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.*».

[85] GDPR art. 37 (Designazione del responsabile della protezione dei dati) «*2. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; …omissis….*».

[86] d. lgs. 51/2018, art. 28 (Designazione del responsabile della protezione dei dati) «*1. Il titolare del trattamento designa un responsabile della protezione dei dati.*».

[87] GDPR art. 38 (Posizione del responsabile della protezione dei dati) «*3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.*».

e l'assenza di conflitti d'interesse (art. 38 par. 6 lett. a GDPR[88]). Già nelle indicazioni del WP29 (Linee guida DPO) e nelle FAQ del Garante sono state indicate situazioni di conflitto di interessi in relazione a ruoli manageriali di vertice come quelli, tra gli altri, di *"[…] responsabile finanziario […] direzione risorse umane, responsabile IT*", di "*responsabile per la prevenzione della corruzione e per la trasparenza*" (Documento di indirizzo DPO punto 10.1).

L'autorità garante italiana si è espressa in maniera netta sul punto affermando che «*Si può certamente affermare la sussistenza di un conflitto di interessi in relazione ai ruoli già citati (come la direzione risorse umane o contabilità, il responsabile IT o il responsabile della prevenzione della corruzione e della trasparenza), trattandosi di settori in cui i trattamenti dei dati personali sono certi e trasversali rispetto all'intera amministrazione, oltre che significativi in termini di quantità e qualità dei dati personali trattati, nonché di rischi sui diritti e sulle libertà fondamentali degli interessati. Peraltro, altre Autorità europee si sono già pronunciate espressamente in proposito (invero con riferimento all'ambito privato), sancendo l'incompatibilità tra la figura di RPD e quella di responsabile IT (provv. dell'Autorità bavarese del 20 ottobre 2016) o quella di dirigente dei dipartimenti che si occupano di conformità normativa, della gestione del rischio e di audit interni (provv. dell'Autorità belga n. 18/2020 del 28 aprile 2020)*» (Documento di indirizzo DPO punto pag. 32).

Nel sistema oggetto della presente valutazione è stato nominato responsabile della protezione dei dati personali (RDP/DPO) Giuseppe Nuzzolese, presso Municipio di Santeramo in Colle, piazza dottor Simone, 8 - Santeramo in Colle (BA), soggetto interno.

B1.2.5 EVENTUALI RESPONSABILI DEL TRATTAMENTO (RISCHIO §15)

Il ruolo di responsabile del trattamento (art. 4 par. 8 e art. 28 GDPR, art. 18 d. lgs. 51/2018, Linee guida titolare p. 76, pag. 28), definito anche *Data Processor* (DP), può essere attribuito alle persone fisiche o giuridiche, pubbliche o private, che siano **distinte dal titolare e non siano soggette alla sua autorità e controllo diretto**, questo è l'elemento distintivo rispetto al personale del titolare del trattamento, e **trattino i dati per conto del titolare e nell'ambito delle sue finalità**, questo è l'elemento distintivo rispetto al ruolo di contitolare del trattamento.

La nomina a questo ruolo deve essere formalizzata con **uno specifico contratto in forma scritta o elettronica**, noto come accordo di responsabilità del trattamento o *data processing agreement* (DPA), altro elemento che rende la nomina inapplicabile al personale dipendente dal titolare, il quale deve indicare espressamente le finalità e le modalità del trattamento, in particolare la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento (art. 28 par. 3 GDPR[89]), e ciò vale come regola generale estesa anche ai trattamenti che sono esclusi dall'applicazione del GDPR (art. 18 c. 3 d. lgs. 51/2018[90])

Al responsabile del trattamento è consentita una certa autonomia operativa per i **mezzi non essenziali** del trattamento, categoria residuale rispetto ai **mezzi essenziali** del trattamento, che può definire solo il titolare, che sono strettamente legati alla finalità e alla portata del trattamento, tra cui il tipo di dati

---

[88] GDPR art. 38 «*6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi*.».

[89] GDPR art. 28 (Responsabile del trattamento) «*3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento …omissis…*».

[90] d. lgs. 51/2018, art. 18 (Responsabile del trattamento) « *3. L'esecuzione dei trattamenti da parte di un responsabile del trattamento è disciplinata da un contratto o da altro atto giuridico che prevede l'oggetto, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Tale contratto o diverso atto giuridico prevede anche che il responsabile del trattamento: … omissis…*».

personali trattati, la durata del trattamento, le categorie di destinatari e le categorie di interessati (Linee guida titolare p. 40, pag. 16).

Il responsabile del trattamento può nominarne altri (c.d. **sub responsabili del trattamento**) solo previa autorizzazione del titolare e con l'obbligo d'informarlo tempestivamente per qualsiasi variazione possa intervenire in modo che possa eventualmente opporsi (art. 28 par. 2 GDPR[91] e art. 18 c. 2 d. lgs. 51/2018).

L'accountability e quindi la responsabilità conseguente del titolare è in funziona anche della verifica delle competenze e delle garanzie che offre il responsabile del trattamento per l'attuazione di misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR. Gli elementi di cui tenere conto potrebbero essere le conoscenze specialistiche del responsabile del trattamento (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), il grado di affidabilità, le risorse di cui dispone il responsabile e l'adesione di quest'ultimo a un codice di condotta o a un meccanismo di certificazione riconosciuti.

Allo stato attuale si è rilevato che **sono svolti trattamenti di dati per conto del titolare** (art. 28 par. 3 GDPR e art. 17 c. 2 d. lgs. 51/2018) da parte di Gestione Servizi s.p.a., sebbene **in maniera irregolare**.

B1.2.6 EVENTUALI TRATTAMENTI ESTERNALIZZATI (RISCHIO§16)

L'esternalizzazione, detta anche outsourcing dei beni o servizi relativi alla gestione dei dati personali, può configurare due situazioni differenti sul piano giuridico della normativa sulla protezione dei dati:

- **affidamento della fornitura di beni o servizi necessari alla gestione dei dati** da parte del titolare senza che il trattamento, in alcun caso o in alcun modo prevedibile, possa essere svolto da altri, come ad esempio il noleggio di strumenti di videosorveglianza, la fornitura del servizio di posizionamento degli stessi o la mera manutenzione o assistenza tecnica relativa agli apparati; in questi casi non si configurano le ipotesi di responsabilità o contitolarità del trattamento;
- **affidamento di parti del trattamento dei dati personali**, che si configura in tutti i casi in cui l'esternalizzazione del trattamento non sia esplicito, ma comunque prevedibile, e riguardi anche quantità minime di dati, con riferimento alla quantità o al periodo di trattamento, casi tipici sono il servizio di data entry, la postalizzazione della corrispondenza o delle notifiche delle sanzioni amministrative e cartelle esattoriali per conto del titolare, il controllo o la selezione delle immagini fisse o in movimento riprese dai sistemi di videosorveglianza fissi o mobili, l'archiviazione in cloud o in archivi fisici dei dati trattati dal titolare; in tutti questi casi il soggetto esterno è sempre da considerare responsabile o contitolare del trattamento.

In entrambi i casi, l'affidamento esterno di attività strumentali al trattamento dei dati da parte del titolare devono essere valutato attentamente nell'ottica della conformità alla vigente normativa sulla protezione dei dati (compliance) e della valutazione e gestione del rischio del trattamento (risk management e risk evaluation) valutando in particolare:

- **l'effettiva necessità**, poiché l'affidamento esterno della fornitura di beni e servizi strumentali al trattamento dei dati, nell'ottica del principio di minimizzazione, deve costituire una scelta residuale e inevitabile rispetto tutte le altre opzioni di gestione in proprio (in house);

[91] GDPR art. 28 «*2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.*».

- **il rischio e la proporzionalità**, poiché l'ampliamento della filiera del trattamento fuori dal controllo diretto del titolare costituisce una fonte potenziale di rischio che deve essere attentamente valutata e gestita;
- **la qualificazione giuridica dell'affidamento** nell'ambito della normativa sulla protezione dei dati e questo aspetto non è meramente formale ma sostanziale, poiché la configurazione di un rapporto di responsabilità o di contitolarità nel trattamento dei dati fa conseguire gli adempimenti necessari a carico di ogni soggetto e ripartisce le responsabilità tra di loro.

Il titolare ha dichiarato che sono stati esternalizzati alcuni servizi, in particolare la Gestione Servizi s.p.a.: gestione dei procedimenti sanzionatori per le infrazioni al Codice della Strada, incluso il data entry, le notificazione CAD e CAN, i pagamenti e le sanzioni accessorie, e ha dichiarato altresì che **si è svolta preventivamente la valutazione dei rischi derivanti dalla gestione esterna** di parte del trattamento (art. 25 GDPR e art. d. lgs 51/2018).

B1.2.7 EVENTUALE TRASFERIMENTO DEI DATI IN PAESI TERZI (RISCHIO §17)

I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE)[92], ovvero verso organizzazioni internazionali sono consentiti a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 par. 1 GDPR[93]) e ciò vale anche per i trattamenti esclusi dal campo di applicazione del GDPR (art. 32 d. lgs. 51/2018[94]).

In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 par. 1 GDPR[95] e Raccomandazione trasferimenti) che possono essere:

senza autorizzazione da parte del Garante (art. 46 par. 2 GDPR[96] e art. 33 d. lgs. 51/2018):

- gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a GDPR e art. 33 c. 1 lett. a d. lgs. 51/2018) o la valutazione del titolare, sotto la sua responsabilità,

---

[92] Lo Spazio Economico Europeo deriva da un accordo del 1994 che estende le disposizioni applicate al mercato interno dall'Unione europea ai paesi dell'Associazione europea di libero scambio (EFTA): Norvegia, Liechtenstein, Islanda.

[93] GDPR art. 45 (Trasferimento sulla base di una decisione di adeguatezza) «*1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.*».

[94] d. lgs. 51/2018, art. 16 (Trasferimento sulla base di una decisione di adeguatezza) «*1. Il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale è consentito se la Commissione europea ha deciso che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale garantiscono un livello di protezione adeguato. In tal caso non sono necessarie autorizzazioni specifiche.*».

[95] GDPR art. 46 (Trasferimento soggetto a garanzie adeguate) «*1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.*».

[96] GDPR art. 46 «*2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo: a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; b) le norme vincolanti d'impresa in conformità dell'articolo 47; c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.*».

sulla sussitenza di garanzie adeguate, in questo caso è fatto obbligo di avviso al Garante (art. 33 c. 1 lett. b d. lgs. 51/2018);

- *binding corporate rules* (BCR) ossia le norme vincolanti d'impresa (art. 47 GDPR) approvate dal Garante (art. 46, par. 2, lett. b GDPR);
- *standard contractual clauses* (SCC) ossia le clausole contrattuali standard (CCS) definite dalla Commissione europea e da inserire integralmente (art. 46, par. 2, lett. c e lett. d GDPR);
- *codes of conduct* ossia i codici di condotta (art. 46, par. 2, lett. e GDPR);
- i meccanismi di certificazione (art. 46, par. 2, lett. f GDPR).

previa autorizzazione dell'Autorità Garante (art. 46 par. 3 GDPR[97]):

- le clausole contrattuali ad hoc (art. 46, par. 3, lett. a GDPR);
- gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b GDPR).

In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe che si verificano in specifiche situazioni (art. 49 GDPR[98] e art. 34 d. lgs. 51/2018) tra le quali:

- consenso informato dell'interessato (art. 49 par. 1 lett. a GDPR e art. 34 d. lgs. 51/2018);
- trasferimento necessario per l'esecuzione di un contratto concluso tra il titolare (DC) e l'interessato (DS) al trattamento (art. 49 par. 1 lett. b GDPR) ovvero da altro soggetto in favore dell'interessato (art. 49 par. 1 lett. c GDPR);
- rilevanti motivi di interesse pubblico (art. 49 par. 1 lett. d GDPR) o per prevenire una minaccia grave e immediata alla sicurezza pubblica (art. 34 c. 1 lett. c d. lgs. 51/2018);
- trasferimento necessario per l'esercizio di un diritto giudiziario (art. 49 par. 1 lett. e GDPR e art. 34 c. 1 lett. e d. lgs. 51/2018);
- trasferimento necessario per la tutela di interessi vitali dell'interessato o di altri soggetti laddove l'interessato sia nell'incapacità di esprimere il consenso (art. 49 par. 1 lett. f GDPR e art. 34 c. 1 lett. a d. lgs. 51/2018).

---

[97] GDPR art. 46 «*3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1: a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.*».

[98] GDPR art. 49 (Deroghe in specifiche situazioni) «*1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni: a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; d) il trasferimento sia necessario per importanti motivi di interesse pubblico; e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.*».

Il titolare ha dichiarato che, alla data della presente valutazione, il trattamento oggetto di questa valutazione **non comporta trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali**. Il titolare si impegna a riesaminare la presente valutazione prima dell'eventuale attivazione di servizi cloud, manutenzioni da remoto, piattaforme software o sub-responsabili che possano comportare accesso ai dati da Paesi terzi.

B1.2.8 CATEGORIE DI INTERESSATI E TIPOLOGIE DI DATI TRATTATI (RISCHIO §18)

Il Comune di Santeramo in Colle attraverso i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale tratta le immagini fisse e le riprese video, cronodatate e geolocalizzate, delle persone e dei veicoli che transitano nel raggio d'azione delle telecamere e specificatamente:

categorie di interessati: utenti e cittadini, autori di violazioni amministrative, autori di reati, conducenti e passeggeri di veicoli, personale dipendente in via accidentale;

tipologie di dati trattati:

a) **dati identificativi**: *targa e dati dei veicoli*;

b) **categorie particolari di dati** (art. 9 GDPR e art. 7 d. lgs. 51/2018): *nessuna*.

Il titolare ha dichiarato che **non sono trattate categorie particolari di dati** e quindi non si rilevano rischi da approfondire e verificare su questo punto.

B1.2.9 EVENTUALE PARERE DEGLI INTERESSATI E STANDARD APPLICABILI (RISCHIO §19)

Parere degli interessati

Per le finalità di prevenzione, indagine, accertamento e perseguimento di reati, attività ausiliaria di salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 5 l. 65/1986 e art. 57 c.p.p.), con particolare riferimento alla sicurezza urbana (l. 48/2017) non è stato richiesto il parere degli interessati essendo funzioni escluse dall'applicazione del GDPR (art. 2 par. 2 lett. d GDPR) e per le quali non è richiesto (art. 5 c. 1 d. lgs. 51/2018).

Per i trattamenti finalizzati agli scopi istituzionali dell'ente, compresa la polizia amministrativa, l'accertamento delle violazioni amministrative (art. 13 l. 689/81) e l'attività di polizia stradale (art. 11 CdS), , il parere degli interessati non è stato richiesto poiché il fondamento giuridico è l'assolvimento di obblighi di legge e funzioni di interesse pubblico (art. 6 par. 1 lett. e GDPR).

Sebbene la norma consenta l'accertamento delle violazioni con ogni forma (art.13 legge 689/81) e non definisca le modalità tecniche con le quali esercitare le qualifiche di legge attribuite alla Polizia Locale, tuttavia nessuna norma impone o comunque prevede esplicitamente, anche come mera facoltà, l'utilizzo della videosorveglianza per assolvere a questi obblighi di legge e funzioni di interesse pubblico, pertanto appare opportuno richiedere in qualsiasi forma possibile il parere degli interessati che si consiglia vivamente.

Standard applicabili al trattamento

La standardizzazione (o unificazione o normalizzazione o normazione) è una metodologia con la quale vengono fissate le caratteristiche di un insieme di prodotti o procedure in modo tale che siano comparabili i loro aspetti fondamentali, appunto standard, ad esempio di qualità, funzionalità, affidabilità, senza dover specificare le singole caratteristiche e senza dover valutare ogni singolo caso, ma accettando quelle fornite dalla categoria standardizzata. Ad esempio a livello internazionale l'International Organization for Standardization (ISO) definisce norme e procedure per certificare prodotti e procedure, come nel caso della qualità dei processi definita dalla ISO 9001.

Nel caso della protezione dei dati la presenza di eventuali standard permette di assicurare la conformità del trattamento alle norme sulla protezione dei dati e l'accountability del titolare. Essi sono definiti esplicitamente dalla normativa nelle categorie generali dei:

- **codici di condotta** (art. 40 GDPR[99]);
- **meccanismi di certificazione** (art. 42 GDPR[100]).

Questi strumenti trovano applicazione solo nell'ambito di applicazione materiale del GDPR poiché non vi sono analoghe previsioni nella disciplina nazionale (Codice della privacy, d. lgs. 51/2018).

Per la tipologia dei trattamenti valutati in questo atto quindi non si possono applicare finalità del trattamento in oggetto come si può rilevare dal registro nazionale ed europeo all'indirizzo https://www.gpdp.it/codici-di-condotta e inoltre non esistono standard di certificazione per i trattamenti di dati personali in generale e in particolare per questi trattamenti, ma solo e specificatamente per quanto attiene alla sicurezza informatica e alla cybersecurity (ISO/IEC 27001:2022) anche con riferimento alla privacy, che comunque è uno strumento utile e da apprezzare laddove adottato dal titolare.

In via generale, nel trattamento valutato in questo atto il titolare segue le privacy policies indicate nel Registro dei trattamenti e le indicazioni date dalle Linee guida del EDPB e dal Garante italiano per la protezione dei dati personali. Si ribadisce la **necessità di adottare idonei atti normativi e organizzativi aggiornati** e in particolare le Linee guida sul trattamento dei dati.

B1.2.10 ESATTEZZA, AGGIORNAMENTO DEI DATI E DELLA VALUTAZIONE (RISCHIO §20)

I dati oggetto di trattamento devono essere, per principio, esatti e aggiornati ed eventualmente corretti, sia a richiesta dell'interessato (DS) e sia d'iniziativa del titolare (DC), adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (art. 5 p. 1 lett. d GDPR[101]).

Al fine della verifica della correttezza del trattamento, da cui ne deriva la corretta acquisizione, mantenimento e aggiornamento della base dati, dei processi di rettifica dei dati inesatti e dell'eliminazione dei dati non necessari, si ritiene che anche la presente valutazione d'impatto-DPIA costituisca uno strumento di accountability, da verificare e aggiornare secondo le indicazioni e le scadenze riportate nelle conclusioni alla presente sezione.

Si rileva che la valutazione d'impatto è stata rinnovata dopo oltre 30 giorni dalla scadenza che era fissta per il 6/3/2025 Si raccomanda di rinnovare la presente valutazione prima del termine di scadenza del prossimo 3/2/2027.

---

[99] GDPR art. 40 (Codici di condotta) «*1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.[…omissis…]*».

[100] GDPR art. 42 (Certificazione) «*1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese..[…omissis…]*».

[101] Reg. (UE) UE 2016/679 GDPR, art. 5: «*1 I dati personali sono: [...] d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");*».

B1.3 Criticità della sezione 1 e quantificazione del rischio

Trattamento preso in considerazione (rischio §11)

Il trattamento non è organizzato da alcun atto e quindi è necessario provvedere al più presto ad adottare un disciplinare (art. 24 p. 1 GDPR) che preveda anche adeguate misure di sicurezza (art. 32 GDPR).

CALCOLO DEL RISCHIO §11	Indice potenziale di magnitudo	2,00	Indice stimato di pericolo	0,50

Soggetti di riferimento per il trattamento (rischio §12)

I soggetti di riferimento per il trattamento sono definiti e nominati secondo i documenti che sono stati forniti, tuttavia la carenza di un disciplinare sul trattamento dei dati (art. 24 p. 1 GDPR), che si è valutato nel rischio precedente, può costituire un pregiudizio nella definizione effettiva dei ruoli del trattamento e delle loro funzioni.

CALCOLO DEL RISCHIO §12	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Eventuali contitolari del trattamento (rischio §13)

Al momento non è in vigore alcun trattamento congiunto dichiarato dal titolare.

CALCOLO DEL RISCHIO §13	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Responsabile per la protezione dei dati (rischio §14)

Non emergono particolari rischi per quanto riguarda il responsabile della protezione dei dati personali (RDP/DPO).

CALCOLO DEL RISCHIO §14	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Eventuali responsabili del trattamento (rischio §15)

Non è stato sottoscritto l'accordo di responsabilità del trattamento-DTA ai sensi della vigente normativa (art. 28 par. 3 GDPR e art. 18 d. lgs. 51/2018) e ciò può incidere gravemente sulla sicurezza del trattamento.

CALCOLO DEL RISCHIO §15	Indice potenziale di magnitudo	2,00	Indice stimato di pericolo	1,00

Eventuali trattamenti esternalizzati (rischio §16)

Non si rilevano particolari rischi.

CALCOLO DEL RISCHIO §16	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Eventuale trasferimento di dati in paesi terzi (rischio §17)

Non sono eseguiti trasferimenti di dati personali in paesi terzi e pertanto non sussistono rischi.

CALCOLO DEL RISCHIO §17	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Tipologie di dati trattati (rischio §18)

Sono definite chiaramente le tipologie di dati e le categorie d'interessati, non sono trattate categorie particolari di dati (art. 9 GDPR e art. 7 d. lgs. 51/2018), non si rilevano quindi particolari rischi.

CALCOLO DEL RISCHIO §18	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Eventuale parere degli interessati e standard applicabili (rischio §19)

Per le finalità e le modalità del trattamento svolto si può derogare dal parere degli interessati, quindi non si rilevano particolari rischi. Per le finalità e la tipologia del trattamento non sono disponibili standard da applicare.

CALCOLO DEL RISCHIO §19	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Esattezza, aggiornamento dei dati e della valutazione (rischio §20)

La presente valutazione d'impatto è stata rinnovata a oltre 30 giorni dalla precedente scadenza (6/3/2025) e ciò costituisce un rischio marginale ma da evitare per la sicurezza del trattamento. Si raccomanda di rinnovare la presente valutazione sempre prima del termine di scadenza.

CALCOLO DEL RISCHIO §20	Indice potenziale di magnitudo	2,00	Indice stimato di pericolo	0,50

B1.4 Piano di riduzione del rischio della sezione 1

Per ridurre il rischio del nuovo trattamento di cui alla presente valutazione d'impatto-DPIA, si segnala al titolare del trattamento e al RPD/DPO l'opportunità di rimediare in tempi brevi, nel rispetto dei principi di accountability (art. 24 GDPR) e di legalità e correttezza dei trattamenti per finalità di polizia (art. 15 d. lgs. 51/2018), alle criticità evidenziate nel paragrafo precedente.

Fermo restando la piena autonomia del titolare, si suggeriscono alcune attività che potrebbero essere adottate in tempi brevi e da verificare entro la prossima revisione della presente valutazione-DPIA, fissata fra 180 giorni ossia entro il 3/2/2027.

Sezione B1-Descrizione generale del trattamento oggetto della DPIA		**Risk mitigation**
RISCHIO	**MISURE DI MITIGAZIONE DEL RISCHIO**	
§11	*adozione di un disciplinare sul trattamento dei dati (art. 24 p. 1 GDPR) che preveda anche adeguate misure di sicurezza (art. 32 GDPR);*	
§12	*nessuna necessaria;*	
§13	*nessuna necessaria;*	
§14	*nessuna necessaria;*	
§15	*stipula di specifico contratto tra titolare e responsabili del trattamento;*	
§16	*nessuna necessaria;*	
§17	*nessuna necessaria;*	
§18	*nessuna necessaria;*	
§19	*nessuna necessaria;*	
§20	*nessuna necessaria.*	
Indice di vulnerabilità stimato (Vu§1): 0,25-adeguate		

B1.5 Calcolo del rischio della sezione 1

Il rischio complessivo, con le procedure e i riferimenti indicati in precedenza, in attesa di ulteriore verifica alla prossima valutazione d'impatto, che consenta di stimare la vulnerabilità del sistema durante il funzionamento, all'esito dell'applicazione delle misure proposte per la riduzione del rischio e delle ulteriori che saranno adottate di propria iniziativa dal titolare, anche sulla base di eventuali indicazioni del responsabile per la protezione dei dati personali (RPD/DPO), risulta come segue:

Sezione B1-Descrizione generale del trattamento oggetto della DPIA				**Risk evaluation**
RISCHIO	**ELEMENTO VALUTATO**	**MAGNITUDO**	**PERICOLO**	
§11	Trattamento preso in considerazione	2,00	0,50	
§12	Soggetti di riferimento per il trattamento	0,00	//	
§13	Eventuali contitolari del trattamento	0,00	//	
§14	Responsabile per la protezione dei dati	0,00	//	
§15	Eventuali responsabili del trattamento	2,00	1,00	
§16	Eventuali trattamenti esternalizzati	0,00	//	
§17	Eventuali trasferimenti in paesi terzi	0,00	//	
§18	Tipologie di dati trattati	0,00	//	
§19	Eventuale parere degli interessati e standard applicabili	0,00	//	
§20	Esattezza, aggiornamento dei dati e della valutazione	2,00	0,50	
Rischio emergente della sezione (Re§1)		5,00(*)	2,50(*)	**12,50-alto**
Indice di vulnerabilità (Vu§1)	0,25	**Rischio residuo (Rr§1)**		**3,13-medio**
Parere del RPD/DPO:		*vedasi eventuale giudizio allegato.*		
Giudizio del titolare del trattamento (DC):		*vedasi giudizio finale.*		

(*) Il rischio è limitato al valore massimo di 5 sia per la magnitudo e sia per il pericolo.

Sezione B2-Valutazione della necessità, proporzionalità e legittimità del trattamento

B2.1 Premessa sul principio di necessità e proporzionalità

B2.1.1 PRINCIPIO DI NECESSITÀ

La normativa europea sulla protezione dei dati personali di cui al GDPR non definisce espressamente il principio di necessità che è una conseguenza del principio di minimizzazione dei dati, il quale impone che i dati siano "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*" (art. 5 par. 1 lett. c GDPR).

Da ciò derivano più piani di valutazione del criterio di necessità:

- **necessità sostanziale**: i dati personali dovrebbero essere trattati solo se la finalità del trattamento non sono ragionevolmente conseguibili con altri mezzi (considerando 39);
- **necessità essenziale**: nei casi in cui si debbano trattare categorie particolari di dati (art. 9 GDPR) senza il consenso dell'interessato, ciò è possibile a condizione che ricorrano particolari forme di necessità essenziali e tassativamente previste ossia:
    - per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (art. 9 p. 2 lett. c GDPR) ovvero per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale (art. 9 p. 2 lett. h GDPR);
    - per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9 p. 2 lett. b GDPR);
    - per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali (art. 9 p. 2 lett. f GDPR);
    - per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9 par. 2 lett. g GDPR).
- **necessità temporale**: i dati personali devono essere conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica (considerando 39) e conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (art. 5 par. 1 lett. e GDPR).

B2.1.2 AMBITI PARTICOLARI DI ATTUAZIONE DEL PRINCIPIO DI NECESSITÀ

Il principio di necessità per le finalità di prevenzione e repressione dei reati, controllo delle minacce all'ordine e alla sicurezza pubblica, attività escluse dal campo di applicazione GDPR e alle quali assolve in parte il sistema di videosorveglianza, è definito molto più semplicemente che negli altri

casi come la necessità di svolgere una funzione per la quale l'autorità pubblica è competente (art. 5 c. 1 d. lgs. 51/2018[102]).

Per circoscrivere il campo di applicazione di questa definizione la legge inizialmente rimandava a successivo regolamento di esecuzione e poi (decreto-legge n. 139/2021 convertito con modificazioni dalla legge n. 205/2021) ha rimesso la competenza a decreti del Ministro dell'interno e del Ministro della giustizia l'individuazione dei trattamenti o delle categorie di trattamenti non occasionali per i quali è considerato sussistente il principio di necessità e quindi la liceità degli stessi, definendo anche i termini e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione e le condizioni per l'esercizio dei diritti degli interessati (art. 5 c. 2 d. lgs. 51/2018[103]).

B2.1.3 PRINCIPIO DI PROPORZIONALITÀ

Il principio di proporzionalità nel trattamento dei dati personali deriva dal principio generale fissato dal Trattato sull'Unione europea che pone la proporzionalità come limite a tutte le competenze comunitarie e quindi anche all'attività normativa (art. 5 c. 1 T.U.E.[104]).

Nel trattamento dei dati personali, la proporzionalità impone che la liceità delle azioni trovi come limite generale quanto strettamente necessario per il conseguimento degli obiettivi (art. 5 c. 4 T.U.E.[105]) quindi non eccedenti rispetto ai mezzi e le modalità e da ciò ne derivano in particolare il principio di minimizzazione dei dati e di limitazione della conservazione.

B2.1.4 CRITERIO DI VALUTAZIONE SEGUITO

Nella valutazione d'impatto-DPIA si deve considerare la proporzionalità di tutti i singoli trattamenti in relazione alle loro effettiva finalità (art. 35 par. 7 lett. b GDPR[106]) e implicitamente anche la necessità.

Inoltre, considerando che il fine perseguito non giustifica in assoluto i mezzi impiegati per conseguirlo, il trattamento sarà valutato in relazione al rapporto rischio/beneficio e si considererà accettabile solo quando non sia possibile ricorrere ad altro sistema meno invasivo sui dati personali e sulla libertà degli interessati[107].

---

[102] d. lgs. 51/2018, art. 5 (liceità del trattamento) «*1. Il trattamento è lecito se è necessario per l'esecuzione di un compito di un'autorità competente per le finalità di cui all'articolo 1, comma 2, e si basa sul diritto dell'Unione europea o su disposizioni di legge o, nei casi previsti dalla legge, di regolamento che individuano i dati personali e le finalità del trattamento.*».

[103] d. lgs. 51/2018, art. 5 «*2. Con decreto rispettivamente, del Ministro della giustizia e del Ministro dell'interno, sono individuati, per i trattamenti o le categorie di trattamenti non occasionali di cui al comma 1, i termini, ove non già stabiliti da disposizioni di legge o di regolamento, e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti di cui agli articoli 9, 10, 11 e 13. I termini di conservazione sono determinati in conformità ai criteri indicati all'articolo 3, comma 1, tenendo conto delle diverse categorie di interessati e delle finalità perseguite.*».

[104] Trattato sull'Unione europea (versione consolidata), art. 5: «*1. La delimitazione delle competenze dell'Unione si fonda sul principio di attribuzione. L'esercizio delle competenze dell'Unione si fonda sui principi di sussidiarietà e proporzionalità.*».

[105] Trattato sull'Unione europea (versione consolidata), art. 5: «*4. In virtù del principio di proporzionalità, il contenuto e la forma dell'azione dell'Unione si limitano a quanto necessario per il conseguimento degli obiettivi dei trattati.*».

[106] Reg. (UE) 2016/679 GDPR, art.35: «*7. La valutazione contiene almeno:[...]b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;[...]*».

[107] EDPB-European Data Protection Board. Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Versione 2.1 26 febbraio 2020, punto 1.5 «*La videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che ci si prefigge. Altrimenti si rischia di modificare le norme culturali con la conseguenza di ammettere come regola l'assenza di privacy.*».

B2.1.5 ELEMENTI VALUTATI IN QUESTA SEZIONE

1) **ambito territoriale e proporzionalità dei mezzi impiegati;**
2) **specificazione delle finalità e base giuridica del trattamento;**
3) **necessità del trattamento per finalità amministrative;**
4) **conformità del trattamento per finalità di polizia;**
5) **conformità delle riprese sui luoghi di lavoro;**
6) **legittimi interessi e bilanciamento dei diritti;**
7) **minimizzazione e termine di conservazione delle immagini;**
8) **automatismi e profilazione;**
9) **conformità dell'eventuale trattamento con bodycam;**
10) **conformità dell'eventuale trattamento con droni**.

B2.2 Valutazione della necessità e proporzionalità del trattamento

B2.2.1 AMBITO TERRITORIALE E PROPORZIONALITÀ DEI MEZZI IMPIEGATI (RISCHIO §21)

Caratteristiche geografiche e demografiche del territorio

Comune di Santeramo in Colle [*fonte dati ISTAT anno 2025*]:
- altezza media sul livello del mare: 489 m;
- estensione territoriale: 144,38 km^2;
- popolazione residente: 25.735 abitanti;
- densità: 178,24 abitanti/km^2.

Polizia Locale [*dati forniti dal titolare del trattamento*]:
- operatori totali: 19;
- ufficiali: 4 compreso il ;
- turni di servizio giornalieri: 2.

Indici della criminalità del contesto territorialedati riferiti al territorio della Città Metropolitana di Bari [*fonte dati Sole 24Ore Indici della criminalità anno 2024*]:

a) **CRIMINALITÀ COMPLESSIVA**
   - posizione nella classifica delle province con maggiore criminalità: **29° posizione in Italia**;
   - numero complessivo di denunce: 44.416,0;
   - denunce ogni 100.000 abitanti: 3.631,4.

b) **OMICIDI**
   - omicidi denunciati: 2;
   - omicidi ogni 100.000 abitanti: 0,2;
   - posizione nella classifica delle province per numero di omicidi: **90° posizione in Italia**.

c) **RAPINE**
   - rapine denunciate: 399,0;
   - rapine ogni 100.000 abitanti: 32,6;
   - posizione nella classifica delle province per quantità di rapine: **32° posizione in Italia**.

d) FURTI

- furti denunciati: 19.821,0;
- furti ogni 100.000 abitanti: 1.620,6;
- posizione nella classifica delle province per quantità di furti: **23° posto in Italia**.

Secondo l'ANCI-Associazione Nazionale dei Comuni Italiani [Fonte dati: ANCI pubblicazione *"Rapporto Nazionale sull'attività della Polizia Locale*" anno 2023], che prende in esame 145 comuni tra capoluoghi di provincia e città con oltre 50.000 abitanti, nelle aree urbane italiane vivono 19.848.879 persone e sono installate 29.137 telecamere, con un rapporto medio di 1 telecamera ogni 681 abitanti; gli operatori della polizia locale sono stati censiti nel numero complessivo di 27.098, con un rapporto quindi di 1 operatore ogni 732 abitanti.

Il territorio dell'Italia è si estende su una superficie di 302.068,3 km^2 [fonte dati: www.istat.it dati al 1 gennaio 2024], il territorio urbanizzato è pari al 19,30% della superficie complessiva [Fonte dati: ISTAT "Forme, livelli e dinamiche dell'urbanizzazione in Italia, anno 2017] quindi le aree urbane hanno una superficie complessiva di 58.299 km^2, considerate le telecamere complessivamente installate in Italia secondo le stime ANCI precedentemente citate ne consegue quindi che il rapporto medio nelle aree urbane è di 1 telecamera ogni 2,00 km^2.

Il territorio del Comune di Santeramo in Colle, come si è già indicato, si estende su una superficie di 144,38 km^2 e, secondo i dati dell'ultimo censimento, conta una popolazione residente di 25.735 abitanti, gli operatori della Polizia Locale sono 19 tra i quali vi sono 4 ufficiali (funzionari direttivi categoria D) incluso il ; i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale allo stato consistono di 54 punti di ripresa, dei quali 4 di tipo mobile, che per la loro caratteristica di precarietà non saranno considerati nella presente valutazione di proporzionalità.

Su questi dati risultano i seguenti rapporti in ordine al numero di telecamere impiegate a livello locale e nazionale:

- 1 telecamera ogni 477 abitanti (media italiana 1 telecamera ogni 681 abitanti);
- 1 telecamera ogni 2,67 km^2 di territorio (media italiana 1 telecamera ogni 2,00 km^2).

TABELLA COMPARATIVA TELECAMERE/TERRITORIO

	Italia	**Comune di Santeramo in Colle**	
Numero telecamere	**28.233** (dati ANCI 2023)	**54**	
Abitanti nelle aree urbane	**18.799.800** (dati ANCI 2023)	**25.735**	
Superficie aree urbane	**58.299** km^2 (dati ISTAT 2024)	**144,38** km^2	**Δ Comune di Santeramo in Colle/Italia**
Abitanti per telecamera	**690** abitanti per TLC	**477** abitanti per TLC	**+30%**
Superficie per telecamera	**2,00** km^2 per TLC	**2,67** km^2 per TLC	**-34%**

Il rapporto tra il numero di punti di ripresa del sistema valutato in questo atto e la popolazione mostra valori superiori alle medie nazionali rilevate da ANCI (30%) e nella valutazione di questo valore si deve tenere conto anche del contesto territoriale della sicurezza e delle risorse a disposizione per gestirla, considerato anche il ridotto numero di operatori di polizia locale che è inferiore alle medie nazionali delle statistiche ANCI (-84,91%), che quindi non riesce a vigilare adeguatamente sulla sicurezza dei cittadini.

Il rapporto tra il numero di telecamere e l'estensione del territorio mostra valori inferiori del -34% alle medie delle aree urbane nazionali rilevate da ANCI (-34%) e ciò evidenzia l'attenzione del titolare al bilanciamento degli interessi, si deve considerare anche il ridotto numero di operatori di polizia locale che, come si è detto in precedenza, è inferiore alle medie nazionali ANCI, che quindi non riesce a presidiare adeguatamente il territorio nella sua estensione.

Si rende comunque necessario verificare costantemente l'effettiva necessità e proporzionalità dei mezzi impiegati e delle aree sottoposte a trattamento dei dati mediante i sistemi di videosorveglianza, come si farà negli aggiornamenti periodici del presente documento.

B2.2.2 SPECIFICAZIONE DELLE FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO (RISCHIO §22)

Secondo il principio della limitazione della finalità (art.5 p. 1 lett. b GDPR[108]), la legittimità del trattamento è in funzione degli scopi che si vogliono perseguire che, in ogni fase del trattamento, devono essere leciti, determinati, espliciti e legittimi.

Il trattamento valutato in questo documento è quello svolto con i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale, **non risultano compiutamente definite o comunque esplicitate** anche perché manca un atto organizzativo generale dell'ente (ex art. 24 p. 1 GDPR) per completare la base giuridica del trattamento (art. 2-ter c. 1-bis Codice della Privacy).

Per le finalità di esercizio di pubblici poteri provvede la Polizia Locale in virtù delle qualifiche di agente o ufficiale di polizia giudiziaria (art. 5 c. 1 lett. a l. 65/1986[109] e art. 57 c.p.p.[110]), acquisita ope legis da tutti gli operatori, e della qualifica di agente di pubblica sicurezza (art. 5 c. 1 lett.c l. 65/1986[111]), ottenuta per riconoscimento da parte del prefetto (art. 5 c. 2 L. 65/1986[112]).

---

[108] Reg. (UE) UE 2016/679 GDPR, art. 5: «*1. I dati personali sono: [...] b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");*».

[109] Legge 65/1986, art. 5 (Funzioni di polizia giudiziaria, di polizia stradale, di pubblica sicurezza): «*1. Il personale che svolge servizio di polizia municipale, nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni, esercita anche: a) funzioni di polizia giudiziaria, rivestendo a tal fine la qualità di agente di polizia giudiziaria, riferita agli operatori, o di ufficiale di polizia giudiziaria, riferita ai responsabili del servizio o del Corpo e agli addetti al coordinamento e al controllo,[...] omissis…*».

[110] Codice di procedura penale, art. 57 (Ufficiali e agenti di polizia giudiziaria): «*1. Salve le disposizioni delle leggi speciali, sono ufficiali di polizia giudiziaria:...omissis… c) il sindaco dei comuni ove non abbia sede un ufficio della polizia di Stato ovvero un comando dell'arma dei carabinieri o della guardia di finanza. 2. Sono agenti di polizia giudiziaria:...omissis… b) i carabinieri, le guardie di finanza, gli agenti di custodia, le guardie forestali e, nell'ambito territoriale dell'ente di appartenenza, le guardie delle province e dei comuni quando sono in servizio. 3. Sono altresì ufficiali e agenti di polizia giudiziaria, nei limiti del servizio cui sono destinate e secondo le rispettive attribuzioni, le persone alle quali le leggi e i regolamenti attribuiscono le funzioni previste dall'articolo 55.*».

[111] Legge 65/1986. art. 5: «*1. Il personale che svolge servizio di polizia municipale, nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni, esercita anche:...omissis… c) funzioni ausiliarie di pubblica sicurezza ai sensi dell'articolo 3 della presente legge.*».

[112] Legge 65/1986. art. 5: «*2. A tal fine il prefetto conferisce al suddetto personale, […omissis…], la qualità di agente di pubblica sicurezza, dopo aver accertato il possesso dei seguenti requisiti[...] omissis…*».

Queste funzioni sono svolte anche dai dipendenti del Comune di Santeramo in Colle ai quali è riconosciuta la qualifica di polizia stradale (art. 12 e 12-bis C.d.S., art. 5 c. 1 lett. a l. 65/1986[113]) o di polizia amministrativa (art. 13 legge 689/81[114]).

Il principio di liceità del trattamento (art. 6 GDPR par. 1[115]; art. 3 c. 1 lett. a e art. 5 d. lgs. 51/2018) prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica, tassativamente prevista, che può essere:

- **consenso dell'interessato** (art. 6 par. 1 lett. a GDPR e considerando 32, 42, 43) che può essere implicito o esplicito (art. 7 GDPR);
- **adempimento degli obblighi contrattuali** (art. 6 par. 1 lett. b GDPR);
- **adempimento di obblighi legali ai quali è soggetto il titolare** (art. 6 par. 1 lett. c GDPR e considerando 45; art. 5 c. 1 d. lgs. 51/2018);
- **salvaguardia degli interessi vitali dell'interessato o di altra persona fisica** (art. 6 par. 1 lett. d GDPR e considerando 46);
- **interesse pubblico o esercizio di pubblici poteri** (art. 6 par. 1 lett. e GDPR);
- **interesse legittimo** prevalente del titolare o di terzi cui i dati vengono comunicati (art. 6 par. 1 lett. f GDPR e considerando 47, 48).

Il Codice della Privacy[116] (art. 2-ter c. 1[117] e art. 2-ter c. 1-bis Codice della Privacy[118]) ha esteso anche alle fonti secondarie il fondamento giuridico dei trattamenti, da intendersi come espressione di

---

[113] Legge 65/1986, art. 5 (Funzioni di polizia giudiziaria, di polizia stradale, di pubblica sicurezza): «*1. Il personale che svolge servizio di polizia municipale, nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni, esercita anche:...omissis… b) servizio di polizia stradale,… omissis…*».

[114] Legge 689/81, art. 13 (Atti di accertamento): «*1. Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro...omissis... 4. All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria, ...omissis... 5. È fatto salvo l'esercizio degli specifici poteri di accertamento previsti dalle leggi vigenti.*».

[115] Reg. (UE) UE 2016/679 GDPR, art. 6 (Liceità del trattamento): «*1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è 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; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.*».

[116] Il d. l. 139/2021 (c.d. decreto capienze) ha modificato l'art. 2-ter del Codice della privacy ha esteso ai regolamenti, anche se non immediatamente previsti dalla fonte primaria, e agli atti amministrativi generali il fondamento della base giuridica del trattamento.

[117] D. lgs. 196/2003, art. 2-ter «*1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita esclusivamente da una norma di legge o di regolamento o da atti amministrativi generali*».

[118] D. lgs. 196/2003, art. 2-ter «*1-bis. 1-bis. Il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi comprese le Autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonché da parte di una società a controllo pubblico statale di cui all'articolo 16 del decreto legislativo 19 agosto 2016, n. 175, con esclusione per le società pubbliche dei trattamenti correlati ad attività svolte in regime di libero mercato, è sempre consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti. La finalità del trattamento, se non espressamente prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento, è indicata dall'amministrazione, dalla società a controllo pubblico in coerenza al compito svolto o al potere esercitato, assicurando adeguata pubblicità all'identità del titolare del trattamento, alle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano*».

"*potestà amministrativa*" rivolta alla "*cura concreta di interessi pubblici, con effetti diretti nei confronti di una pluralità di destinatari non necessariamente determinati nel provvedimento, ma determinabili*" (Cass. civ. Sez. Unite, 28 novembre 1994, n. 10124) e che "*esprime una scelta di carattere essenzialmente tecnico, con cui l'amministrazione persegue la cura degli interessi pubblici a essa affidati dalla legge*" (Corte Cost., 22 luglio 2010, n. 278).

Quindi, in tutti i casi nei quali le finalità del trattamento non siano disciplinate dalla legge, le pubbliche amministrazioni possono fornire con proprio atto normativo la base giuridica del trattamento ma non in maniera indiscriminata, poiché la stessa norma prevede che tale finalità debba essere necessaria per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri a essa attribuiti, assicurando adeguata pubblicità all'identità del titolare del trattamento, alle finalità del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.

BASE GIURIDICA DEI TRATTAMENTI SVOLTI DAL TITOLARE

BASE GIURIDICA	FINALITÀ DEL TRATTAMENTO
consenso dell'interessato (art. 6 p. 1 lett. a GDPR)	//
adempimento di obblighi contrattuali (art. 6 p. 1 lett. b GDPR)	//
adempimento di obblighi legali (art. 6 p. 1 lett. c GDPR)	//
salvaguardia di interessi vitali (art. 6 p. 1 lett. d GDPR)	//
assolvimento di compiti o interessi pubblici ed esercizio di pubblici poteri (art. 6 p. 1 lett. e GDPR; art. 1 c. 1 lett. d. lgs. 51/2018), funzione di polizia giudiziaria, amministrativa e pubblica sicurezza (art. 5 l. 65/1986 e art. 2-ter d. lgs. 196/2003), , approvato con n. del (art. 2-ter d. lgs. 196/2003)	//
prevenzione, indagine, accertamento e perseguimento di reati e minacce alla pubblica sicurezza (art. 1 c. 2 d. lgs. 51/2018; art. 1 c. 1 lett. d. lgs. 51/2018), funzione di polizia giudiziaria, amministrativa e pubblica sicurezza (art. 5 l. 65/1986 e art. 2-ter d. lgs. 196/2003)	prevenzione, indagine, accertamento e perseguimento di reati, attività ausiliaria di salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 5 l. 65/1986 e art. 57 c.p.p.), con particolare riferimento alla sicurezza urbana (l. 48/2017);
perseguimento di interessi legittimi (art. 6 p. 1 lett. f GDPR)	non applicabile in quanto autorità pubblica (art. 6 p. 1 GDPR).

Per queste specifiche finalità il Comune di Santeramo in Colle, non avendo competenza a disciplinare con proprie norme (art. 118[119] Cost.) la materia dell'ordine e della sicurezza pubblica così come l'attività giurisdizionale, di competenza esclusiva dello Stato (art. 117[120] Cost.), si limita a definire le

[119] Costituzione art. 118: «*1. Le funzioni amministrative sono attribuite ai Comuni salvo che, per assicurarne l'esercizio unitario, siano conferite a Province, Città metropolitane, Regioni e Stato, sulla base dei principi di sussidiarietà, differenziazione ed adeguatezza. I Comuni, le Province e le Città metropolitane sono titolari di funzioni amministrative proprie e di quelle conferite con legge statale o regionale, secondo le rispettive competenze.…omissis…*».

[120] Costituzione art. 117: «*1. La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali. Lo Stato ha legislazione esclusiva nelle seguenti*

modalità del trattamento solo in via subordinata e residuale rispetto alla legge e ai decreti del Ministero dell'interno e della Giustizia che definiscono i termini, le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti (art. 5 c. 2 d. lgs. 51/2018[121]).

Nel trattamento analizzato in questo documento la presenza di sistemi ANPR che mantengono nella memoria tutte le targhe di passaggio, anche di quelle che non hanno commesso violazioni amministrative, costituisce un'attività che rende opportuno un accordo con l'autorità di PS.

B2.2.3 NECESSITÀ DEL TRATTAMENTO PER FINALITÀ AMMINISTRATIVE (RISCHIO §23)

Per le finalità di polizia amministrativa dei trattamenti svolti attraverso i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale, attività che sono ricomprese nel campo di applicazione del regolamento (UE) 2016/679 (art. 2 p. 1 GDPR), il principio di necessità richiede di dimostrare che tali finalità non siano ragionevolmente conseguibili con altri mezzi (considerando 39[122]). Laddove fossero trattate categorie particolari di dati (art. 9 GDPR) si deve dimostrare che sussista una necessità essenziale che può essere esclusivamente la tutela di interessi vitali (art. 9 p. 2 lett. c GDPR), finalità di medicina del lavoro (art. 9 p. 2 lett. h GDPR), diritto del lavoro e della sicurezza e protezione sociale (art. 9 p. 2 lett. b GDPR), esigenze giurisdizionali (art. 9 p. 2 lett. f GDPR), motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9 p. 2 lett. g GDPR).

In questo caso la necessità deriva dalle dimensioni del Comune di Santeramo in Colle, che si estende su una superficie di 144,38 km^2 con una popolazione residente di 25.735 abitanti, rapportate all'esiguo numero di operatori di polizia dell'ente che sono 19, con un rapporto di 1 operatore ogni 1.354 abitanti, -84,91% rispetto la media nazionale rilevata da ANCI di 1 operatore ogni 732 abitanti, gli unici competenti ad assolvere queste finalità in virtù della qualifiche di polizia stradale (art. 5 c. 1 lett. a l. 65/1986 e art. 12 C.d.S.) e di polizia amministrativa (art. 13 l. 689/1981).

---

materie:...omissis… h) ordine pubblico e sicurezza, ad esclusione della polizia amministrativa locale;...omissis… l) giurisdizione e norme processuali; ordinamento civile e penale; giustizia amministrativa;...omissis…».

[121] d. lgs. 51/2018, art. 5: «*2. Con decreto, rispettivamente, del Ministro della giustizia e del Ministro dell'interno, sono individuati, per i trattamenti o le categorie di trattamenti non occasionali di cui al comma 1, i termini, ove non già stabiliti da disposizioni di legge o di regolamento, e le modalità di conservazione dei dati, i soggetti legittimati ad accedervi, le condizioni di accesso, le modalità di consultazione, nonché le modalità e le condizioni per l'esercizio dei diritti di cui agli articoli 9, 10, 11 e 13....omissis…*».

[122] Reg. (UE) 2016/679 GDPR, considerando 39: «*Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.*».

Il numero degli ufficiali, necessari per il coordinamento dell'attività sul territorio, è in questo caso, e di 1 ufficiale/funzionario direttivo ogni 6.434 abitanti, -50,46% rispetto la media nazionale rilevata da ANCI di 1 ufficiale/funzionario direttivo ogni 4.276 abitanti.

TABELLA COMPARATIVA POLIZIA LOCALE/TERRITORIO

	Principali Corpi di Polizia Locale	Polizia Locale di Santeramo in Colle	
Numero operatori di Polizia Locale	**27.098** (dati ANCI 2023)	**19**	
Numero ufficiali di Polizia Locale	**4.642** (dati ANCI 2023)	**4**	
Abitanti nelle aree urbane	**19.848.879** (dati ANCI 2023)	**25.735**	**Δ Polizia Locale di Santeramo in Colle/Italia**
Abitanti per operatore	**732**	**1.354**	**-84,91%**
Abitanti per ufficiali	**4.276**	**6.434**	**-50,46%**

La necessità del trattamento del sistema di videosorveglianza per questa finalità risulta dimostrata e argomentata, considerato anche che non sono trattate categorie particolari di dati (art. 9 GDPR).

B2.2.4 CONFORMITÀ DEL TRATTAMENTO PER FINALITÀ DI POLIZIA (RISCHIO §24)

In via generale, per le finalità di prevenzione e repressione dei reati, controllo delle minacce all'ordine e alla sicurezza pubblica, la necessità del trattamento è quella di svolgere una funzione per la quale l'autorità pubblica è competente ed obbligata (art. 5 c. 1 d. lgs. 51/2018) ed è esclusa dal campo di applicazione del regolamento (UE) 2016/679 (art. 2 p. 2 lett. d GDPR, art. 1 c. 1 d. lgs. 51/2018) applicandosi viceversa il decreto legislativo 51/2018 che ha recepito la direttiva (UE) 2016/680.

I trattamenti che perseguono queste finalità devono essere conformi, in particolare, alle modalità indicate dal regolamento di cui al D.P.R. 15/2018 che, per i sistemi di videosorveglianza, impone una **necessità specifica** per le finalità di polizia, **proporzionalità** che escluda ingerenze ingiustificate nei diritti e nelle libertà fondamentali delle persone interessate (art. 22 D.P.R. 15/2018[123]) e minimizzazione dei dati che limiti i dati delle persone identificabili (art. 24 c. 1 D.P.R. 15/2018[124]).

Nel caso specifico del Comune di Santeramo in Colle la necessità deriva dall'assolvimento delle funzioni di polizia giudiziaria e di pubblica sicurezza che competono agli operatori di polizia dell'ente, che rivestono ope legis la qualifica di agente o ufficiale di polizia giudiziaria (art. 5 c. 1 lett. a l. 65/1986 e art. 57 c.p.p.) e di agente di pubblica sicurezza (art. 5 c. 1 lett. c l. 65/1986). Nei

[123] D.P.R. 15/2018, art. 22 (Sistemi di videosorveglianza): «*1. L'utilizzo di sistemi di videosorveglianza è consentito ove necessario per le finalità di polizia di cui all'articolo 3 e a condizione che non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate. 2. Gli organi, uffici e comandi di polizia, nel rispetto dei principi richiamati dagli articoli 4, 5 e 6, raccolgono solo i dati strettamente necessari per il raggiungimento delle finalità di cui all'articolo 3, registrando esclusivamente le immagini indispensabili.*».

[124] D.P.R. 15/2018, art. 24 (Speciali misure di sicurezza relative al trattamento di dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video): «*1. I sistemi informativi e i programmi informatici destinati alla registrazione e alla conservazione dei dati personali raccolti attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video, sono configurati, in conformità al criterio di necessità del trattamento dei dati personali di cui all'articolo 5, in modo da ridurre al minimo l'utilizzazione di dati relativi a persone identificabili.*».

successivi aggiornamenti della presente valutazione d'impatto-DPIA si verificherà la sussistenza della situazione qui accertata suggerendo, nel caso, agli opportuni adeguamenti.

Per tutti i casi in cui la videosorveglianza sia utilizzata per le finalità di prevenzione e repressione dei reati, controllo delle minacce all'ordine e alla sicurezza pubblica sono richieste **speciali misure di sicurezza** per garantire la sicurezza del trattamento (art. 24 c. 2-6 D.P.R. 15/2018[125]):

- **livelli diversificati di accesso** di visibilità e trattamento delle immagini da parte degli incaricati del trattamento che gli consentano di svolgere i soli compiti assegnati (art. 24 c. 2 D.P.R. 15/2018);
- **misure contro gli accessi abusivi** per tutelare le immagini riprese contro i rischi di manomissione o di visualizzazione non autorizzata (art. 24 c. 3 D.P.R. 15/2018);
- **registrazione in file log mantenuti per 5 anni** degli accessi e delle operazioni eseguite dagli operatori abilitati (art. 24 c. 4 D.P.R. 15/2018);
- **log accessibili solo per controllo** della liceità del trattamento, del controllo interno e per garantire l'integrità e la sicurezza dei dati personali e nell'ambito dei procedimenti penali (art. 24 c. 5 D.P.R. 15/2018).

Le misure di sicurezza specifiche che sono prescritte dalla normativa per i trattamenti con finalità di prevenzione, accertamento e repressione dei reati e delle minacce all'ordine e alla sicurezza pubblica (art. 24 c. 2 D.P.R. 15/2018) nel caso oggetto della presente valutazione risultano gravemente carenti mancando degli aspetti fondamentali ossia: livelli diversificati di accesso, misure contro gli accessi abusivi, registrazione attività in file log mantenuti per 5 anni, log accessibili solo per controllo.

B2.2.5 CONFORMITÀ DELLE RIPRESE SUI LUOGHI DI LAVORO (RISCHIO §25)

I sistemi di videosorveglianza negli ambienti di lavoro possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza dei lavoratori e per la tutela del patrimonio aziendale e in questi casi vanno osservate le garanzie previste dalla legge (art. 4 Statuto dei lavoratori[126] e art. 2 d. lgs. n. 165/2001). Lo statuto dei lavoratori vieta infatti il controllo a distanza dei dipendenti sia all´interno degli edifici e sia in altri luoghi di prestazione di lavoro, ad esempio le telecamere installate sui veicoli non devono riprendere in modo stabile la postazione di guida e le immagini possono essere utilizzate per accertare e perseguire eventuale illeciti penali ma non per controlli, anche indiretti, sull´attività dei conducenti, e non consente l´installazione di sistemi di

[125] D.P.R. 15/2018, art. 24: «*2. Sono adottati diversificati livelli di visibilità e di trattamento delle immagini da parte degli incaricati del trattamento i quali sono autorizzati, attraverso il rilascio di credenziali di autenticazione, a compiere le sole operazioni di trattamento correlate ai compiti assegnati. 3. Sono adottate specifiche misure di sicurezza contro i rischi di accesso abusivo di cui all'articolo 615-ter del codice penale nei confronti degli apparati di ripresa digitale utilizzati ai fini della registrazione delle immagini qualora connessi a reti informatiche. 4. Gli accessi e le operazioni, effettuati dagli operatori abilitati in relazione ai sistemi informativi di cui al comma 1, sono registrati in appositi file di log, non modificabili, che sono conservati per cinque anni dall'accesso o dall'operazione. Sono fatti salvi i diversi termini di conservazione previsti da speciali disposizioni. 5. Gli accessi ai file di log di cui al comma 4 sono consentiti ai soli fini della verifica della liceità del trattamento, del controllo interno, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito del procedimento penale. 6. Ai trattamenti di dati personali che implicano maggiori rischi di un danno alla persona interessata in ragione della natura dei dati, delle modalità del trattamento o degli effetti che esso può determinare, si applica la disposizione di cui all'articolo 6, comma 1.*».

[126] Legge 20 maggio 1970 art. 4 (Impianti audiovisivi e altri strumenti di controllo): «*1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. […omissis…]*».

videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all´attività lavorativa, come ad esempio in bagni, spogliatoi, docce, armadietti e luoghi ricreativi.

In tutti i casi nei quali per le finalità lecite sopra indicate, le telecamere siano installate negli ambienti di lavoro in senso stretto o nelle immediate prossimità, laddove ci sia comunque la possibilità di controllare l'attività dei lavoratori, è richiesto un atto formale preliminare che deve acquisire il datore di lavoro che sia titolare del trattamento e precisamente:

- **accordo collettivo** stipulato dalla **rappresentanza sindacale unitaria (RSU)** o dalle **rappresentanze sindacali aziendali (RSA)**, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale;
- in mancanza di accordo deve essere richiesta **autorizzazione** alla **sede territoriale dell'Ispettorato nazionale del lavoro (UTL)**, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'**Ispettorato nazionale del lavoro**.

Eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull´attività giornalistica, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l´osservanza del codice deontologico per l´attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi anche, per motivi legittimi, alla sua diffusione.

Nel sistema valutato in questo documento **la legittimità delle telecamere installate negli ambienti di lavoro o nelle loro prossimità, attualmente spente, richiede accordo sindacale** ovvero autorizzazione della sede competente per territorio dell'Ispettorato nazionale del lavoro prima che esse siano attivate.

B2.2.6 LEGITTIMI INTERESSI E BILANCIAMENTO DEI DIRITTI (RISCHIO §26)

Il trattamento può essere considerato lecito e quindi possibile anche senza chiedere il consenso dell'interessato ovvero senza che sia fondato su altre basi giuridiche (adempimento di obblighi contrattuali o legali, salvaguardia di interessi vitali, assolvimento di compiti o interessi pubblici ed esercizio di pubblici poteri) laddove si possa dimostrare la sussistenza di un legittimo interesse del titolare o di terzi e a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (art. 6 p. 1 lett. f GDPR[127]).

L'esigenza di trattare i dati per questa finalità sorge per le imprese, persone fisiche o giuridiche, per i professionisti e le organizzazioni, nei confronti degli interessati dai quali non hanno acquisito il consenso al trattamento dei loro dati personali ovvero non hanno obblighi legali in genere o l'esigenza di adempiere a obbligazioni negoziali, per finalità di marketing sul proprio target di riferimento, ad esempio per inviare comunicazioni promozionali e informative, per la prevenzione delle frodi, ad esempio nel caso in cui si acquisiscano informazioni precontrattuali sulla solvibilità dei clienti o

[127] Reg. (UE) 2016/679 GDPR, art.6: «*1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: […] f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;[...]*».

sull'affidabilità dei fornitori (considerando 47[128]), ovvero per condividere i dati della clientela o dei dipendenti all'interno di un gruppo imprenditoriale (considerando 48[129]).

In tutti i casi in cui il trattamento sia basato sull'interesse legittimo del titolare, l'interessato ha il diritto di opporsi al trattamento, salvo che l'interessato dimostri motivi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (art. 21 GDPR).

La liceità di questa finalità è fondata sul bilanciamento dei diritti, sussiste quindi l'obbligo per il titolare di verificare e dimostrare, nell'ottica dell'accountability, che i propri legittimi interessi o quelli di terzi - ad esempio quando il trattamento è finalizzato a vendere i dati raccolti ad altre aziende - non prevalga specificatamente su:

- **diritti e le libertà fondamentali** dell'interessato;
- **interessi dell'interessato** tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

Ad esempio nel caso in cui si installino sistemi di videosorveglianza per evitare il rischio di furti o rapine, si dovrà valutare il rischio potenziale per il titolare, che in alcuni casi potrebbe essere elevato come per le banche e le gioiellerie ma non lo è in astratto per tutti, la storia e le statistiche e i casi subiti caso per caso, e, utilizzando proporzionalmente l'interesse del titolare rispetto le effettive esigenze, si potrebbe stabilire di attivare la videosorveglianza solo durante l'orario di chiusura.

Il titolare dovrà non solo valutare se ha correttamente preso in considerazione tutti i rischi per i dati trattati, ma anche raccogliere e documentare – ad esempio nel registro dei trattamenti - elementi sufficienti per comprovare che i contrapposti interessi siano stati correttamente bilanciati tra loro valutando e questa base giuridica sia stata utilizzata con proporzionalità rispetto la necessità, per dimostrare la sua accountability.

Il trattamento oggetto della presente valutazione **non può, in alcun caso, utilizzare come base giuridica il legittimo interesse** in quanto esso il titolare è un'autorità pubblica (art. 6 par. 1 GDPR).

B2.2.7 MINIMIZZAZIONE E TERMINE DI CONSERVAZIONE DEI DATI (RISCHIO §27)

Questo principio impone come comportamento generale che il trattamento sia limitato sempre ai soli dati personali indispensabili, pertinenti, come aspetto qualitativo, e adeguati, in senso quantitativo,

---

[128] Considerando 47 GDPR: « *I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.* ».

[129] Considerando 48 GDPR: «*I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo.*».

per il perseguimento delle finalità per cui sono raccolti e trattati (art. 5 p. 1 lett. c GDPR[130]). In particolare, per i trattamenti attraverso gli strumenti di videosorveglianza che hanno fini di polizia è richiesta espressamente la minimizzazione dei dati delle persone identificabili (art. 24 c. 1 D.P.R. 15/2018).

Prima di installare un sistema di videosorveglianza, il titolare del trattamento deve sempre valutare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata e necessaria per i suoi scopi e si dovrebbe optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato.

Nel trattamento oggetto della presente valutazione d'impatto-DPIA si devono registrano solo le immagini di specifiche porzioni di territorio che siano attinenti e conformi alle finalità del trattamento, pertanto dovranno essere rilevati solo i dati essenziali e, al fine di limitare il quantitativo complessivo di dati trattati, la videosorveglianza interesserà le aree che, in generale, presentano maggiori rischi potenziali ovvero che siano state interessate con frequenze più elevata da eventi che rientrano nelle finalità perseguite dal trattamento quindi, in particolare, le zone che sono più esposte alla criminalità, dove siano stati registrati più illeciti e che siano interessate da fenomeni di degrado (art. 5 c. 2 D.lgs.14/2017).

Le immagini possono essere conservate per termini differenziati secondo le finalità che perseguono.

Le Linee guida videosorveglianza (punto 8.121) chiariscono che le immagini registrate dai sistemi di videosorveglianza devono essere conservate per il tempo strettamente necessario a perseguire le finalità per le quali sono state installate e, di norma fino ad un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o giorni di chiusura oppure indagini di polizia e giudiziarie.

Nella valutazione della proporzionalità del termine per la conservazione dei dati nel trattamento oggetto della presente valutazione d'impatto-DPIA si deve considerare:

- **gli orari di funzionamento degli uffici e i giorni di apertura**, nel Comune di Santeramo in Colle il servizio della Polizia Locale è strutturato su 2 turni, quindi la vigilanza non è assicurata per tutto l'arco della giornata e per tutti i giorni dell'anno;
- **la consistenza numerica del personale** la Polizia Locale ha 19 operatori complessivi con un rapporto rispetto la popolazione di 1 operatore ogni 1.354 abitanti, quindi la carenza di personale non riesce a garantire un'adeguata vigilanza sul territorio per accertare le violazioni alle norme e ad occuparsi tempestivamente della visualizzazione ed estrapolazione dei dati del sistema di videosorveglianza;
- **il tempo necessario per la denuncia dei reati** da parte dei cittadini che ne sono vittime o che ne hanno comunque conoscenza e, quindi, per lo svolgimento dei conseguenti accertamenti dei fatti e acquisizione delle prove dal sistema di videosorveglianza da parte della Polizia Locale ovvero delle altre forze di polizia.

Sulla base di questi parametri il titolare del trattamento, sentito anche il della Polizia Locale, ha definito il termine che segue:

tempo di conservazione dei dati della videosorveglianza:	**7 giorni**

[130] Reg. (UE) UE 2016/679 GDPR, art. 5: «*1. I dati personali sono: [...] c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");*».

Al superamento del termine di conservazione i dati sono cancellati automaticamente mediante sovrascrittura delle immagini più vecchie salvo estrazione e conservazione di porzioni di registrazioni nel caso specifico della denuncia di reati o di minacce all'ordine e alla sicurezza pubblica, in questi casi le immagini delle aree interessate potranno essere conservate per termini maggiori, in conformità alle vigenti norme (art. 10 D.P.R. 15/2018[131]) e secondo le disposizioni dell'autorità giudiziaria.

Il tempo di ritenzione dei dati è entro è entro i 7 giorni e appare adeguatamente motivato, il titolare del trattamento dei dati, al mutare delle esigenze effettive, ridurrà la durata del termine di conservazione.

B2.2.8 AUTOMATISMI E PROFILAZIONE (RISCHIO §28)

Gli automatismi sono algoritmi che valutano i comportamenti umani ai quali applicano risposte con logiche programmate che determinano conseguenze predefinite che, a seconda dei casi, possono essere:

- **fisiche**, quando il comportamento umano rilevato dal sistema determina la variazione di uno stato materiale in conseguenza dell'azionamento di dispositivi elettrici, elettronici, meccanici, ad esempio l'accensione delle luci al passaggio, l'apertura della sbarra di accesso al parcheggio al riconoscimento della targa autorizzata, lo sblocco del cellulare o del pc o l'apertura di una porta al riconoscimento biometrico dell'utente;
- **logiche**, quando il comportamento umano rilevato dal sistema determina la variazione di uno stato immateriale in conseguenza della registrazione di dati in archivi, ad esempio il rilevamento della presenza al lavoro al passaggio nei pressi di dispositivi elettronici che rilevano il badge o il dispositivo RFID, la presenza nelle lezioni online attraverso l'attività al computer;
- **giuridiche**, laddove le scelte automatizzate abbiano conseguenze giuridiche, ad esempio il sanzionamento del veicolo che supera i limiti di velocità o che entra in una zona a traffico limitato.

La normativa in materia di protezione dei dati distingue due categorie di trattamenti automatizzati di dati personali:

- **processi decisionali automatici**, quando vi sono trattamenti basati su decisioni automatizzate che producono effetti giuridici che incidono in modo significativo sull'interessato (art. 22 par. 1 GDPR[132]), inclusa la profilazione;
- **profilazione**, quando si utilizzano trattamenti automatizzati per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze

[131] D.P.R. 15/2018, art.10 (Termini di conservazione dei dati): «*3.[...]u) dati raccolti mediante sistemi di ripresa fotografica audio e video nei servizi di ordine pubblico e di polizia giudiziaria - 3 anni dalla raccolta dati raccolti mediante sistemi di videosorveglianza o di ripresa fotografica audio e video di documentazione dell'attività operativa - 18 mesi dalla raccolta. Si applicano i diversi termini di conservazione di cui alla lettera b) quando i dati personali sono confluiti in un procedimento per l'applicazione di una misura di prevenzione o quelli di cui alle lettere a) f) g) h) e i) quando i dati personali sono confluiti in un procedimento penale.*».

[132] Reg. (UE) UE 2016/679 GDPR, art. 22 (Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione): «*1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*».

personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di persone fisiche (art. 4 par. 1 num. 4 GDPR[133]).

I processi decisionali automatici che non comprendono l'intervento umano nella decisione sono di norma vietati tranne nei casi in cui (art. 22 c. 1 e 2 e considerando 71[134]) sia:

- **necessario per la conclusione o l'esecuzione di un contratto** tra l'interessato e un titolare del trattamento (art. 22 par. 2 lett. a);
- **autorizzato dal diritto dell'Unione o di uno Stato membro** cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato (art. 22 par. 2 lett. b);
- **basato sul consenso esplicito** dell'interessato (art. 22 par. 2 lett. c).

Quindi si deve valutare attentamente ogni processo che preveda decisioni automatizzate e verificarne sia la base giuridica e sia l'adeguata informativa resa all'interessato.

Nel trattamento oggetto della presente valutazione non sono presenti processi decisionali automatizzati.

B2.2.9 CONFORMITÀ DELL'EVENTUALE TRATTAMENTO CON BODYCAM (RISCHIO §29)

Le bodycam sono telecamere indossabili che permettono di riprendere foto, video e audio, archiviandoli nella loro memoria, di quanto sia sostanzialmente nel suo campo visivo frontale dell'operatore che le utilizza.

---

[133] Reg. (UE) UE 2016/679 GDPR, art. 4: «*1. Ai fini del presente regolamento s'intende per:: [...] 4) "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;;*».

[134] GDPR considerando 71 «*L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore. Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.».*

Non essendoci la possibilità di fornire alcuna informativa sul trattamento dei dati, come impone inderogabilmente la normativa sui trattamenti generali dei dati personali (art. 13-14 GDPR), questo sistema di videosorveglianza può essere impiegato solo per quelle finalità che, escluse dal campo di applicazione del GDPR (art. 2 par. 2 lett. d GDPR e art. 1 d. lgs. 51/2018), non richiedono come condizione di liceità del trattamento il consenso dell'interessato e l'informativa sul trattamento dei dati come sono esclusivamente le finalità di prevenzione, indagine, accertamento e perseguimento dei reati e delle minacce alla sicurezza pubblica.

Il principio di necessità che legittima l'impiego di questi dispositivi risiede nell'esigenza di **documentare azioni illecite in un "teatro operativo" particolarmente complesso e ad alto rischio, pertanto l'impiego deve essere motivato caso per caso e non può essere generalizzato**.

L'Autorità Garante, fornendo il proprio parere preventivo (art. 24 d. lgs. 51/2018) alla valutazione d'impatto sulla protezione dei dati-DPIA, presentate rispettivamente dal Ministero dell'Interno-Direzione generale della Polizia di Stato[135] e Arma dei Carabinieri-Comando generale[136], ha precisato e disposto che:

- **è sempre necessaria la valutazione preventiva del Garante sulla DPIA per legittimarne l'impiego**, poiché con le bodycam il trattamento è sempre da considerarsi ad alto rischio (art. 24 c. 1 lett. b del d.lgs. 51/2018)[137];
- **l'impiego delle bodycam deve essere documentato** nei verbali, negli atti di polizia giudiziaria, nelle annotazioni di servizio, con l'identificativo dell'operatore che l'indossa[138].
- **le immagini possono essere conservate al massimo per sei mesi con cancellazione automatica**, salvo il diverso termine fissato nel caso di procedimenti penali[139];
- **devono essere implementate idonee misure di sicurezza e tracciamento degli accessi**.

Nel trattamento in oggetto **non sono presenti telecamere indossabili/body cam** e quindi non si valuta questo rischio.

B2.2.10 CONFORMITÀ DELL'EVENTUALE TRATTAMENTO CON DRONI (RISCHIO §30)

Il termine drone identifica a livello colloquiale tutti gli aeromobili a pilotaggio remoto (APR) o Unmanned Aircraft System (UAS) che individua complessivamente il sistema composto dall'aeromobile, dalla stazione di controllo e dal collegamento con il quale il pilota ed eventualmente anche il navigatore controllano il volo da remoto, sul terreno o in altre posizioni.

---

[135] Autorità Garante per la Protezione dei Dati Personali, provvedimento n. 290 del 22 luglio 2021.

[136] Autorità Garante per la Protezione dei Dati Personali, provvedimento n. 291 del 22 luglio 2021.

[137] Autorità Garante per la Protezione dei Dati Personali, provv. 291/2021 punto 4 pag. 7-8 *«[…omissis…] Pertanto, l'attività di trattamento in discussione va considerata a elevato rischio per gli interessati e, trovando applicazione l'articolo 24, par. 1, lett. a) del Decreto, si ritiene necessaria la consultazione preventiva.»*.

[138] Autorità Garante per la Protezione dei Dati Personali, provv. 291/2021 punto 2.4 pag. 4 *Nelle relazioni di servizio, nei verbali e nelle annotazioni di polizia giudiziaria dovrà essere richiamato il nome del file generato automaticamente dal sistema, recante, tra l'altro, il "CIP" del militare utente e l'identificativo della videocamera.»*.

[139] Autorità Garante per la Protezione dei Dati Personali, provv. 291/2021 punto 6 pag. 8-9 *«[…omissis…] Tutto ciò considerato, il termine di sei mesi indicato nella DPIA quale punto di equilibrio tra le esigenze dell'attività di polizia e quelle di tutela dei dati personali appare ragionevole e rispettoso dei principi previsti dalla disciplina in materia di protezione dei dati personali. Risulta, altresì, rispettato il principio della privacy by default, essendo prevista la cancellazione automatica dei dati personali acquisiti alla scadenza dei sei mesi.»*.

La disciplina vigente[140] attribuisce l'impiego operativo di tali veicoli, ai fini del controllo del territorio per finalità di pubblica sicurezza, con particolare riferimento al contrasto del terrorismo e alla prevenzione dei reati di criminalità organizzata e ambientale, alle forze di polizia statali di cui all'art. 16 della L. 121/81 e quindi alla Polizia di Stato, all'Arma dei Carabinieri, alla Guardia di Finanza e alla Polizia Penitenziaria. Quindi per l'impiego istituzionale degli APR/UAS le altre istituzioni devono ottenere preventivamente **l'equiparazione ad aeromobile di Stato** (art. 746 C.d.N.[141]) per le finalità pubbliche, con provvedimento specifico del Ministero delle Infrastrutture e dei Trasporti, in ogni caso **il trattamento con i droni è sempre da considerarsi trattamento ad alto rischio e quindi si deve inviare preventivamente al Garante la valutazione d'impatto-DPIA anche se impiegati per scopi di polizia** (art. 23 c. 4 DPR 15/2018[142]).

Il titolare del trattamento ha dichiarato che nel sistema valutato in questo atto **non sono presenti trattamenti di dati mediante mezzi di ripresa aerea/droni (APR/UAS)** e quindi non si valuterà questo rischio.

B2.3 Criticità della sezione 2 e quantificazione del rischio

Proporzionalità dei mezzi impiegati (rischio §21)

Il rapporto tra il numero di punti di ripresa e gli abitanti nel Comune di Santeramo in Colle è superiori alle medie nazionali rilevate da ANCI (30%) e nella valutazione di questo valore si deve tenere conto anche del contesto territoriale della sicurezza e delle risorse a disposizione per gestirla; il rapporto tra il numero di telecamere e l'estensione del territorio è inferiore del -34% alle medie delle aree urbanizzate dell'Italiae ciò costituisce un fattore potenziale di rischio marginale che si verificherà negli aggiornamenti del presente documento.

CALCOLO DEL RISCHIO §21	Indice potenziale di magnitudo	0,50	Indice stimato di pericolo	1,00

Specificazione delle finalità e base giuridica del trattamento (rischio §22)

Le finalità del trattamento non risultano compiutamente definite o comunque esplicitate anche perché manca un atto organizzativo generale dell'ente (ex art. 24 p. 1 GDPR) per completare la base giuridica del trattamento (art. 2-ter c. 1-bis Codice della Privacy) e ciò costituisce un rischio rilevante.

CALCOLO DEL RISCHIO §22	Indice potenziale di magnitudo	2,00	Indice stimato di pericolo	1,00

Necessità del trattamento per finalità amministrative (rischio §23)

La necessità è adeguatamente dimostrata e non sono trattate categorie particolari di dati (art. 9 GDPR) quindi non si rilevano particolari rischi.

CALCOLO DEL RISCHIO §23	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

[140] Decreto del Ministero dell'Interno del 13 Giugno 2022 "*Modalità di utilizzo da parte delle Forze di polizia degli aeromobili a pilotaggio remoto*".

[141] Codice della Navigazione, art. 746 (Aeromobili equiparabili a quelli di Stato) «*Salvo quanto disposto dell'articolo 744, quarto comma, il Ministero delle infrastrutture e dei trasporti può, con proprio provvedimento, equiparare agli aeromobili di Stato quegli aeromobili che, pur appartenendo a privati ed essendo da questi esercitati, siano adibiti a un servizio di Stato di carattere non commerciale. Il provvedimento stabilisce limiti e modalità dell'equiparazione ed indica la categoria di aeromobile di Stato cui essa si riferisce. L'equiparazione rende applicabili le disposizioni relative alla categoria cui essa si riferisce e le altre disposizioni indicate nel provvedimento.*».

Conformità del trattamento per finalità di polizia (rischio §24)

Le misure di sicurezza specifiche prescritte (art. 24 c. 2 D.P.R. 15/2018) non sono state attivate e ciò può avere conseguenze molto gravi. all'Autorità Garante

CALCOLO DEL RISCHIO §24	Indice potenziale di magnitudo	2,00	Indice stimato di pericolo	0,50

Conformità delle riprese sui luoghi di lavoro (rischio §25)

Le telecamere installate negli ambienti di lavoro o nelle loro immediate prossimità richiedono l'accordo sindacale prima che siano attivate e ciò costituisce un rischio per la legittimità del trattamento.

CALCOLO DEL RISCHIO §25	Indice potenziale di magnitudo	1,50	Indice stimato di pericolo	1,00

Finalità del trattamento e interessi legittimi (rischio §26)

Le finalità del trattamento sono ben definite e trovano adeguato fondamento giuridico, la base giuridica del trattamento non include gli interessi legittimi e quindi non occorre il bilanciamento degli interessi, pertanto non si rilevano particolari rischi.

CALCOLO DEL RISCHIO §26	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Minimizzazione e termine di conservazione dei dati (rischio §27)

Il periodo di conservazione è entro i 7 giorni e adeguatamente motivato, quindi non si rileva alcun particolare rischio.

CALCOLO DEL RISCHIO §27	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Automatismi e profilazione (rischio §28)

Non sono presenti processi decisionali automatizzati non si rilevano quindi particolari rischi.

CALCOLO DEL RISCHIO §28	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Conformità dell'eventuale trattamento con telecamere indossabili/bodycam (rischio §29)

Nel trattamento in oggetto non sono svolti trattamenti tramite telecamere indossabili/body cam e quindi non si valuta questo rischio.

CALCOLO DEL RISCHIO §29	Indice potenziale di magnitudo	non presenti	Indice stimato di pericolo	//

Conformità dell'eventuale trattamento con sistemi di ripresa aerea/droni (rischio §30)

Nel trattamento in oggetto non sono svolti trattamenti tramite sistemi di ripresa aerea/droni e quindi non si valuta questo rischio.

CALCOLO DEL RISCHIO §30	Indice potenziale di magnitudo	non presenti	Indice stimato di pericolo	//

B2.4 Piano di riduzione del rischio della sezione 2

Per ridurre il rischio del nuovo trattamento di cui alla presente valutazione d'impatto-DPIA, si segnala al titolare del trattamento e al RPD/DPO l'opportunità di rimediare in tempi brevi, nel rispetto dei principi di accountability (art. 24 GDPR) e di legalità e correttezza dei trattamenti per finalità di polizia (art. 15 d. lgs. 51/2018), alle criticità evidenziate nel paragrafo precedente.

Fermo restando la piena autonomia del titolare, si suggeriscono alcune attività che potrebbero essere adottate in tempi brevi e da verificare entro la prossima revisione della presente valutazione-DPIA, fissata fra 180 giorni ossia entro il 3/2/2027.

Sezione B2-Valutazione della necessità, proporzionalità e legittimità		**Risk mitigation**
RISCHIO	**MISURE DI MITIGAZIONE DEL RISCHIO**	
§21	*verifica della effettiva necessità di tutti i punti di ripresa;*	
§22	*adozione di idoneo regolamento sul trattamento dei dati afferente ai casi specifici analizzati nel presente documento;*	
§23	*argomentare compiutamente la necessità del trattamento;*	
§24	*adottare livelli diversificati di accesso, misure contro gli accessi abusivi, registrazione attività in file log mantenuti per 5 anni, log accessibili solo per controllo;*	
§25	*verificare la conformità alla normativa del sistema di videosorveglianza installato sul posto di lavoro;*	
§26	*nessuna necessaria;*	
§27	*nessuna necessaria;*	
§28	*nessuna necessaria;*	
§29	*nessuna necessaria;*	
§30	*nessuna necessaria.*	
Indice di vulnerabilità stimato (Vu§2): 0,25-adeguate		

B2.5 Calcolo del rischio finale della sezione 2

Il rischio complessivo, con le procedure e i riferimenti indicati in precedenza, in attesa di ulteriore verifica alla prossima valutazione d'impatto, che consenta di stimare la vulnerabilità del sistema durante il funzionamento, all'esito dell'applicazione delle misure proposte per la riduzione del rischio e delle ulteriori che saranno adottate di propria iniziativa dal titolare, anche sulla base di eventuali indicazioni del responsabile per la protezione dei dati personali (RPD/DPO), risulta come segue:

Sezione B2-Valutazione della necessità, proporzionalità e legittimità				**Risk evaluation**
RISCHIO	**ELEMENTO VALUTATO**	**MAGNITUDO**	**PERICOLO**	
§21	Proporzionalità dei mezzi impiegati	0,50	1,00	
§22	Specificazione delle finalità e base giuridica del trattamento	2,00	1,00	
§23	Necessità del trattamento per finalità amministrative	0,00	//	
§24	Conformità del trattamento per finalità di polizia	2,00	0,50	
§25	Conformità delle riprese sui luoghi di lavoro	1,50	1,00	
§26	Finalità del trattamento e interessi legittimi	0,00	//	
§27	Minimizzazione e termine di conservazione dei dati	0,00	//	
§28	Automatismi e profilazione	0,00	//	
§29	Conformità dell'eventuale trattamento con telecamere indossabili/bodycam	non presenti	//	
§30	Conformità dell'eventuale trattamento con sistemi di ripresa aerea/droni	non presenti	//	
Rischio emergente della sezione (Re§2)		6,00(*)	3,50(*)	**21,00-alto**
Indice di vulnerabilità (Vu§2)	0,25	**Rischio residuo (Rr§2)**		**5,25-medio**
Parere del RPD/DPO:		*vedasi eventuale giudizio allegato.*		
Giudizio del titolare del trattamento (DC):		*vedasi giudizio finale.*		

(*) Il rischio è limitato al valore massimo di 5 sia per la magnitudo e sia per il pericolo.

Sezione B3-Valutazione del rischio sui diritti e le libertà degli interessati

B3.1 Premessa sull'analisi del rischio a carico degli interessati

B3.1.1 LE FINALITÀ DELL'ANALISI DEL RISCHIO SULLA PROTEZIONE DEI DATI

Come si è già illustrato in precedenza[142], la vigente normativa europea prevede la valutazione d'impatto sulla protezione dei dati personali-DPIA come l'analisi dettagliata dei rischi derivanti dal trattamento che possano influire sui diritti e sulle libertà degli interessati (art.35 p.7 lett. c GDPR)[143]. Corollario di questa finalità è la trasparenza, che non è solo un dovere etico generale ma, soprattutto, uno specifico obbligo giuridico per tutti i trattamenti di dati personali (considerando 39, Linee guida videosorveglianza punto 7).

Quindi in questa sezione si analizzerà nel dettaglio il livello di rischio relativo ai diritti e alle libertà degli interessati dal trattamento oggetto della presente valutazione.

B3.1.2 ELEMENTI VALUTATI IN QUESTA SEZIONE

1) **segnalazione delle postazioni di ripresa;**
2) **contenuto delle informative di primo livello;**
3) **caratteristiche tecniche e posizionamento delle tabelle informative;**
4) **disponibilità delle informative di secondo livello;**
5) **contenuto delle informative di secondo livello;**
6) **acquisizione del consenso degli interessati;**
7) **modalità di esercizio dei diritti degli interessati;**
8) **modalità di applicazione del diritto all'oblio;**
9) **definizione degli obblighi per eventuali responsabile del trattamento;**
10) **protezione dei dati in caso di trasferimento in paesi terzi.**

B3.2 Valutazione delle misure a tutela degli interessati

B3.2.1 SEGNALAZIONE DELLE POSTAZIONI DI RIPRESA (RISCHIO §31)

I soggetti ripresi da qualsiasi sistema di ripresa, ossia gli interessati al trattamento (DS), devono essere consapevoli del fatto che è in funzione un sistema di videosorveglianza ed essere informati sull'estensione dell'area (Linee guida videosorveglianza 7-110 p. 28).

Le finalità del trattamento e le altre informazioni fondamentali devono essere esplicitate attraverso idonea cartellonistica (si veda modello allegato) esplicativa dell'attività di videosorveglianza, definita "***informativa di primo livello***" o "***segnaletica di avvertimento***" (Linee guida videosorveglianza 7.1-112 p. 28) che devono rimandare ad altra fonte contenente tutte le informazioni complete, definita "***informativa di secondo livello***" (Linee guida videosorveglianza 7.2-117 p. 29).

---

[142] Vds. il precedente paragrafo a pag. 13.

[143] Reg. (UE) 2016/679 GDPR, art.35: «*7. La valutazione contiene almeno:[...] c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1 [ndr art.35 c.1: «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,...»];[...]*».

L'informativa di primo livello deve essere posta non in corrispondenza di ogni telecamera ma prima dell'accesso alle aree sottoposte a riprese ovvero nelle vie di accesso, in modo che l'interessato possa scegliere se evitare la sorveglianza o adeguare il proprio comportamento ove necessario (Linee guida videosorveglianza p. 7.1.1-113 pag. 28) in ossequio al principio di correttezza e trasparenza (art. 5 par. 1 lett. a GDPR e art. 3 c. 1 lett. a d. lgs. 51/2018).

Le postazioni di ripresa ove sono installate le telecamere devono essere opportunamente evidenziate mediante cartellonistica contenente vignetta informativa conforme alla normativa vigente (Linee guida videosorveglianza p. 7.1.2-114, pag. 28[144]).

Questo obbligo vale per tutte le tipologie di telecamere.

B3.2.2 CONTENUTO DELLE INFORMATIVE DI PRIMO LIVELLO (RISCHIO §32)

Le informative di primo livello devono fornire informazioni concise, trasparenti, intellegibili e facilmente accessibili (art. 12 par. 5 GDPR), devono essere realizzate secondo il modello definito dal Garante (Linee guida videosorveglianza 7.1.2-115 p. 29) -riportato tra gli allegati del presente atto- e devono contenere le seguenti informazioni essenziali (Linee guida videosorveglianza 7.1.2-114 p. 29):

- **identità del titolare del trattamento (DC) e i recapiti**, in questo: Comune di Santeramo in Colle, piazza Dottor Simone, 8 - 70029 Santeramo in Colle (BA), protocollo@pec.comune.santeramo.ba.it, legale rappresentante sindaco pro tempore;
- **dati di contatto del responsabile per la protezione dei dati/data protection officer (RPD/DPO)**, che sono segreteria@comune.santeramo.ba.it - affarigenerali@pec.comune.santeramo.ba.it;
- **finalità del trattamento,** che in questo caso sono: prevenzione, indagine, accertamento e perseguimento di reati, attività ausiliaria di salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 5 l. 65/1986 e art. 57 c.p.p.), con particolare riferimento alla sicurezza urbana (l. 48/2017);
- **diritti fondamentali degli interessati**;
- **esistenza di interessi legittimi,** in questo caso non ammissibili poiché il titolare del trattamento è autorità pubblica (art. 6 par. 1 GDPR);
- **riferimento all'informativa di secondo livello**, che si raccomanda di inserire su un indirizzo breve e mnemonicamente facile da ricordare, come potrebbe essere https://www.comune.santeramo.ba.itprivacy, da indicare in forma testuale e anche mediante QR-code per favorire l'accessibilità;
- **periodo di conservazione dei dati**, che in questo caso è di 7 giorni;
- **trasferimento di dati a terzi**, che in questo caso non avviene.

[144] European Data Protection Board, Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, punto 7.1.2 (Contenuto delle informazioni di primo livello): «*114. Generalmente, le informazioni di primo livello (segnale di avvertimento) dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento. Si può fare riferimento, ad esempio, ai legittimi interessi perseguiti dal titolare (o da un soggetto terzo) e ai recapiti del responsabile della protezione dei dati (se applicabile). Occorre anche fare riferimento alle informazioni di secondo livello, più dettagliate indicando dove e come trovarle.*».

Il contenuto delle tabelle informative valutate in questo trattamento risulta completo di tutte le informazioni richieste dalla vigente normativa (Linee guida videosorveglianza 7.1.2-114/115).

B3.2.3 CARATTERISTICHE TECNICHE E POSIZIONAMENTO DELLE TABELLE INFORMATIVE (RISCHIO §33)

Il Garante, coordinando il Gruppo di lavoro per la tutela delle persone riguardo al trattamento dei dati personali, si era espresso già nel 2004 sul formato delle tabelle informative da adeguare alle varie ubicazioni (Parere videosorveglianza WP89, punto 7 lett. F[145]), stabilendo che debbano avere un formato e un posizionamento tale da essere chiaramente visibile; il successivo provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010 ha ribadito che le tabelle informative devono avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione (Videosorveglianza provvedimento generale, punto 3.1[146]). Devono essere posizionati ad altezza tale da essere ben visibili e attirare l'attenzione degli avventori, approssimativamente all'altezza degli occhi (Linee guida videosorveglianza 7.1.1-113 p. 28), e realizzati in misura e con caratteri dimensionati in maniera idonea da poter essere leggibili in funzione della velocità di transito della via sulla quale sono applicati.

1. **formato grafico e colori**: il pannello è da realizzare con una forma grafica e con le indicazioni previste dalle Linee guida videosorveglianza, con la dicitura "*Area videosorvegliata*" e contenere il pittogramma della telecamera, il tutto a colori ad alto contrasto;
2. **misura**: da realizzare in materiale plastificato resistente agli agenti atmosferici e ai raggi UV, si consiglia in formato minimo di A4 verticale (l. 210 mm. X h. 297 mm) e A4 orizzontale (l. 297 mm. X h. 210 mm) se posto a un'altezza di 1,70 m. da terra e quindi al livello degli occhi degli interessati ovvero in misura proporzionalmente maggiore al crescere dell'altezza da terra e in funzione del limite di velocità della strada dal quale è visibile;
3. **posizionamento**: in postazione ben visibile, su palo o a muro, prima di tutti gli accessi alle aree sottoposte a videosorveglianza e comunque a distanza e/o posizione tale che il soggetto non sia in alcun modo ripreso prima di aver visualizzato la tabella e che possa leggere agevolmente il contenuto con un visus medio.

Le caratteristiche tecniche e la posizione delle tabelle informative valutate in questo contesto risultano di dimensione inadeguate rispetto la posizione, l'altezza dal suolo e la distanza dal potenziale interessato oggetto di ripresa e, quindi, non svolgono efficacemente la loro funzione secondo le indicazioni della vigente normativa (Parere videosorveglianza WP89, punto 7 lett. F, Videosorveglianza provvedimento generale, punto 3.1, Linee guida videosorveglianza 7.1.1-113).

B3.2.4 DISPONIBILITÀ DELLE INFORMATIVE DI SECONDO LIVELLO (RISCHIO §34)

La normativa europea prevede che l'interessato debba essere messo a conoscenza di ogni trattamento dei suoi dati personali, attraverso informative complete di tutte le informazioni relative al trattamento in atto (art. 13 e 14 GDPR), quando non siano consegnate all'interessato al momento della raccolta

[145] Gruppo di lavoro per la tutela delle persone riguardo al trattamento dei dati personali, parere 4/2004 dell'11/02/2004, punto 7 «F. *[…omissis…] Le finalità della videosorveglianza e il responsabile del trattamento devono essere specificati in tutti i casi. Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni.».*

[146] Garante per la protezione dei dati personali, Videosorveglianza – provvedimento generale del 29/04/2010, punto 3.1 (Informativa) «*Il supporto con l'informativa: -deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera; -deve avere un formato ed un posizionamento tale da essere chiaramente visibile; -può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.».*

dei dati, e che queste debbano essere facilmente accessibili per l'interessato (Linee guida videosorveglianza p. 7.2-117, pag.29[147]).

L'informativa sul trattamento dei dati personali può essere resa in forma scritta, elettronica o orale (art. 12 p. 1 GDPR), quindi anche su una pagina informativa online, il cui indirizzo deve essere chiaramente indicato nell'informativa di primo livello possibilmente anche con un QR. Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in formato non digitale, magari su supporti fisici facilmente leggibili disponibili in punti facilmente accessibili e prossimi all'area videosorvegliata ovvero attraverso un numero telefonico da contattare (Linee guida videosorveglianza p. 7.2-117, pag.29).

Le informative pubblicate sul sito web del titolare devono essere:

- **facilmente accessibili**, (art. 12 p.1 GDPR, Linee guida trasparenza p. 11, pag. 7[148]) quindi l'interessato non deve essere costretto a cercare le informazioni, ma deve essere immediatamente chiaro dove e come queste siano accessibili;
- **stratificate** (Linee guida trasparenza p. 38[149]), ossia organizzate in sezioni tematiche, ad esempio attraverso una landing page privacy che contiene i link alle varie informative per categoria di interessati (dipendenti, utenti dei servizi, privati cittadini, ecc.), in questo modo gli interessati al trattamento che visitano il sito possono avere maggiore trasparenza evitando

[147] European Data Protection Board, Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, punto 7. 2 (Contenuto delle informazioni di primo livello): «*117. Le informazioni di secondo livello devono essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale (sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso. Come sopra illustrato, la segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento a tale secondo livello di informazioni. Inoltre, è preferibile che nelle informazioni di primo livello si faccia riferimento a una fonte digitale (ad esempio, un codice QR o un indirizzo web) per le informazioni di secondo livello. Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in formato non digitale. Dovrebbe essere possibile accedere al secondo livello di informazioni senza entrare nell'area videosorvegliata, soprattutto se le informazioni sono fornite digitalmente (ad esempio, tramite un link). Un altro strumento appropriato potrebbe essere la messa a disposizione di un numero telefonico da contattare. Comunque siano fornite le informazioni, queste devono contenere tutti gli elementi obbligatori a norma dell'articolo 13 del RGPD.*».

[148] Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), versione emendata adottata l'11 aprile 2018, punto 9: « *L'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili, ad esempio perché gli sono fornite direttamente, un link lo dirige verso di esse o le informazioni sono contrassegnate chiaramente oppure perché le informazioni si configurano come risposta a una domanda in linguaggio naturale (ad esempio in una dichiarazione/informativa sulla privacy stratificata online, in FAQ, mediante pop-up contestuali che si attivano quando l'interessato compila un modulo online oppure, in un contesto digitale interattivo, attraverso un'interfaccia chatbot, ecc. Questi meccanismi sono trattati nel dettaglio in seguito, tra cui ai paragrafi 33-40.*».

[149] Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), versione emendata adottata l'11 aprile 2018, punto 38 (Approccio stratificato in ambiente non digitale): «*Un approccio stratificato alla fornitura all'interessato delle informazioni finalizzate alla trasparenza è possibile anche in ambiente offline/non digitale (ad esempio nel mondo reale, come nella comunicazione telefonica o con presenza fisica degli interlocutori), nel quale il titolare del trattamento può scegliere fra varie modalità per facilitare la fornitura delle informazioni (si vedano anche i paragrafi da 33 a 37, 39 e 40 relativamente alle diverse modalità di fornire le informazioni). Quest'approccio non dev'essere confuso con la questione distinta delle dichiarazioni/informative sulla privacy stratificate. Quale che sia il formato utilizzato in quest'approccio stratificato, il Gruppo raccomanda che il primo "strato" (in altre parole, la modalità principale con cui il titolare del trattamento si rivolge inizialmente all'interessato) trasmetta di regola le informazioni più importanti (come indicato al paragrafo 36), vale a dire le finalità del trattamento, l'identità del titolare e una descrizione dei diritti dell'interessato, oltre a informazioni sull'impatto più consistente del trattamento o informazioni sul trattamento che potrebbe cogliere di sorpresa l'interessato. Ad esempio, se il primo contatto con l'interessato avviene telefonicamente, le informazioni potrebbero essere fornite durante la chiamata e, all'insegna del bilanciamento delle informazioni richieste agli articoli 13 e 14, potrebbero essere comunicate con un ulteriore mezzo diverso, ad esempio inviando all'interessato una copia dell'informativa sulla privacy via e-mail e/o un link alla dichiarazione/informativa sulla privacy stratificata online del titolare del trattamento.*».

il "*subissamento informativo*" e completezza di informazioni (Linee guida trasparenza p. 35[150]).

Tutte le informazioni rivolte agli interessati dovrebbero comunque essere disponibili in un unico luogo, fisico a cyber, quindi in un'unica sede e in un unico sito, in un documento completo (in formato digitale o cartaceo), al quale essi possano accedere facilmente qualora intendano consultare nella loro interezza le informazioni di cui sono destinatari, privilegiando la combinazione di metodi elettronici e cartacei, al fine di garantire massima trasparenza e accessibilità.

Il massimo organismo europeo sulla protezione dei dati (EDPB-European Data Protection Board) raccomanda l'utilizzo di tecnologie plurime per fornire informazioni agli interessati, aggiungendo agli obblighi di informativa anche altre informazioni e strumenti, come mappe dinamiche o statiche di geolocalizzazione delle telecamere, app e altri sistemi multimediali che favoriscano da un lato l'identificazione e la specificazione delle fonti video in vista dell'esercizio dei propri diritti e, dall'altro lato, ottenere informazioni più dettagliate sulla tipologia di trattamento (Linee guida videosorveglianza 7.2-118, pag. 30).

Le informative di secondo livello nel sistema oggetto della presente valutazione **non sono facili da trovare e non sono complete e stratificate** secondo quanto previsto dalle norme vigenti (art. 12 p. 1 GDPR, Linee guida videosorveglianza p. 7.2-117 e Linee guida trasparenza p. 35).

B3.2.5 CONTENUTO DELLE INFORMATIVE DI SECONDO LIVELLO (RISCHIO §35)

Le informative di secondo livello devono fornire tutte le informazioni prescritte dalla normativa per i dati che non siano raccolti presso l'interessato (art. 14 GDPR) e, in generale, devono essere concise, trasparenti, intellegibili, formulate con un linguaggio semplice e chiaro, facilmente accessibili (art. 12 par. 1 GDPR e Linee guida trasparenza p. 7, 8, 9 , 10, 11).

In particolare devono essere rese disponibili le seguenti informazioni essenziali (art. 13 e 14 GDPR):

- **identità e i dati di contatto del titolare del trattamento (DC) o del suo rappresentante**, (art. 14 p. 1 lett. a GDPR) che in questo caso sono: Comune di Santeramo in Colle, piazza Dottor Simone, 8 - 70029 Santeramo in Colle (BA), protocollo@pec.comune.santeramo.ba.it, legale rappresentante sindaco pro tempore;
- **dati di contatto del responsabile per la protezione dei dati/data protection officer (RPD/DPO) e i recapiti**, (art. 14 p. 1 lett. b GDPR) che in questo caso sono segreteria@comune.santeramo.ba.it - affarigenerali@pec.comune.santeramo.ba.it;
- **finalità del trattamento e base giuridica del trattamento**, (art. 14 p. 1 lett. c GDPR) che in questo caso sono: ;

[150] Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), versione emendata adottata l'11 aprile 2018, punto 35 (Stratificazione in ambiente digitale e dichiarazioni/informative sulla privacy stratificate): «*Alla luce della quantità d'informazioni da fornire all'interessato, in ambiente digitale il titolare del trattamento può seguire un approccio stratificato, optando per una combinazione di metodi al fine di assicurare la trasparenza. Per evitare un subissamento informativo, il Gruppo raccomanda in particolare l'impiego di dichiarazioni/informative sulla privacy stratificate per collegare le varie categorie d'informazioni da fornire all'interessato, piuttosto che l'inserimento di tutte le informazioni in un'unica informativa sulla schermata. L'approccio stratificato può aiutare a superare la tensione tra completezza e comprensione, nello specifico consentendo agli utenti di muoversi direttamente verso la sezione della dichiarazione/informativa che vogliono leggere. Va notato che le dichiarazioni/informative sulla privacy non sono mere pagine annidiate in altre che richiedono diversi clic per arrivare all'informazione voluta: il design e il layout del primo strato della dichiarazione/informativa sulla privacy dovrebbe essere tale da offrire all'interessato una panoramica chiara delle informazioni a sua disposizione su trattamento dei dati personali e del luogo e del modo in cui può trovarle fra i diversi strati. Un altro aspetto importante è la coerenza delle informazioni sia fra i diversi strati di una siffatta informativa sia all'interno di ogni singolo strato.*».

- **categorie di dati personali trattati**, (art. 14 p. 1 lett. d GDPR) che in questo caso sono: dati personali identificativi (art. 4 GDPR): targa e dati dei veicoli;
- **eventuali destinatari o categorie di destinatari dei dati personali**, (art. 14 p. 1 lett. e GDPR) che in questo caso sono: Gestione Servizi s.p.a.;
- **eventuali trasferimenti in paesi terzi**, (art. 14 p. 1 lett. f GDPR) che in questo caso 02;
- **periodo di conservazione dei dati**, (art. 14 p. 2 lett. a GDPR) che in questo caso è di 7 giorni;
- **esistenza di interessi legittimi**, (art. 14 p. 2 lett. b GDPR) in questo caso nessuno poiché non sono ammessi in quanto autorità pubblica (art. 6 par. 1 GDPR);
- **diritti degli interessati** (art. 14 p. 2 lett. c/d GDPR) e in particolare esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati e inoltre il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
- **il diritto di proporre ricorso all'autorità di controllo**, (art. 14 p. 2 lett. e GDPR) che per l'Italia è: Garante per la Protezione dei Dati Personali, piazza Venezia n. 11 – 00187 Roma, email protocollo@gpdp.it, pec protocollo@pec.gpdp.it;
- **la fonte da cui hanno origine i dati**, (art. 14 p. 2 lett. f GDPR) che in questo caso provengono dagli interessati, attraverso i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale e dagli accertamenti svolti dalla Polizia Locale;
- **l'esistenza di un processo decisionale automatizzato compresa la profilazione**, (art. 14 p. 2 lett. g GDPR) in questo trattamento non sono presenti processi decisionali automatizzati di alcun tipo.

Inoltre si deve utilizzare un sistema comunicativo che sia:

- **conciso e trasparente**, (art. 12 p.1 GDPR, Linee guida trasparenza p. 8, pag. 6[151]) questo implica che siano fornite solo le informazioni essenziali sopra indicate, senza ulteriori elementi e con un linguaggio essenziale e preciso, poiché l'eccesso di informazioni o di parole produce un "*subissamento informativo*" che riduce l'efficacia dell'informativa;
- **stratificato**, (Linee guida trasparenza p. 38, pag. 18) predisponendo informative specifiche per tipologia di trattamento, senza costringere quindi a scorrere ampie porzioni di testo alla ricerca di un argomento in particolare;
- **intellegibile**, (art. 12 p.1 GDPR, Linee guida trasparenza p. 9, pag. 6[152]) che impone di fornire tutte le informazioni fondamentali e sopra indicate con un linguaggio semplice e chiaro che sia comprensibili a un esponente medio del pubblico cui sono dirette.

[151] Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), versione emendata adottata l'11 aprile 2018, punto 7: «*L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica che il titolare del trattamento presenti le informazioni/comunicazioni in maniera efficace e succinta al fine di evitare un subissamento informativo. Tali informazioni dovrebbero essere differenziate nettamente da altre che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d'uso. Nell'ambiente online l'utilizzo di una dichiarazione/informativa sulla privacy stratificata consentirà all'interessato di consultarne immediatamente la specifica sezione desiderata, senza dover scorrere ampie porzioni di testo alla ricerca di un argomento in particolare.*».

[152] Gruppo di lavoro articolo 29, Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (wp260rev.01), versione emendata adottata l'11 aprile 2018, punto 9: « *L'obbligo di fornire informazioni "intelligibili" implica che risultino comprensibili a un esponente*

Le informative di secondo livello presenti in questo trattamento, nelle copie fornite dal titolare, **risultano conformi alla normativa vigente** secondo i parametri di valutazione sopra indicati.

B3.2.6 CONTENUTO DELLE INFORMATIVE PER I TRATTAMENTI DI POLIZIA (RISCHIO §36)

Nel caso dei trattamenti esclusi dal GDPR, finalizzati alla prevenzione, accertamento, repressione dei reati e delle minacce alla sicurezza pubblica hanno obblighi differenti dai trattamenti generali, il titolare da obblighi differenziati in funzione delle informazioni da fornire all'interessato:

a) devono essere rese disponibili, anche sul proprio sito internet, le seguenti informazioni essenziali (art. 10 c. 1 d. lgs. 51/2018):
   - **identità e i dati di contatto del titolare del trattamento (DC) o del suo rappresentante**, (art. 10 c. 1 lett. a d. lgs. 51/2018) che in questo caso sono: Comune di Santeramo in Colle, piazza Dottor Simone, 8 - 70029 Santeramo in Colle (BA), protocollo@pec.comune.santeramo.ba.it, legale rappresentante sindaco pro tempore;
   - **dati di contatto del responsabile per la protezione dei dati/data protection officer (RPD/DPO) e i recapiti**, (art. 10 c. 1 lett. b d. lgs. 51/2018) che in questo caso sono segreteria@comune.santeramo.ba.it - affarigenerali@pec.comune.santeramo.ba.it;
   - **finalità del trattamento**, (art. 10 c. 1 lett. c d. lgs. 51/2018) che in questo caso è ; art. 1 c. 1 lett. d. lgs. 51/2018), funzione di polizia giudiziaria, amministrativa e pubblica sicurezza (art. 5 l. 65/1986 e art. 2-ter d. lgs. 196/2003);
   - **il diritto di proporre ricorso all'autorità di controllo**, (art. 10 c. 1 lett. d d. lgs. 51/2018) che per l'Italia è: Garante per la Protezione dei Dati Personali, piazza Venezia n. 11 – 00187 Roma, email protocollo@gpdp.it, pec protocollo@pec.gpdp.it;
   - **diritti degli interessati** (art. 10 c. 1 lett. e d. lgs. 51/2018) e in particolare esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati e inoltre il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

b) devono essere forniti all'interessato le seguenti informazioni essenziali (art. 10 c. 2 d. lgs. 51/2018):
   - **base giuridica del trattamento** (art.10 c. 2 lett. a d. lgs. 51/2018), funzione di polizia giudiziaria, amministrativa e pubblica sicurezza (art. 5 l. 65/1986 e art. 2-ter d. lgs. 196/2003);
   - **periodo di conservazione dei dati** (art.10 c. 2 lett. b d. lgs. 51/2018), che nel trattamento oggetto di questa valutazione è di 7 giorni oppure il periodo necessario allo svolgimento delle attività previste dalla legge penale e dalle norme sulla pubblica sicurezza;

---

medio del pubblico cui sono dirette. L'intelligibilità è strettamente connessa all'obbligo di utilizzare un linguaggio semplice e chiaro. Il titolare dei dati responsabilizzato saprà su che tipo di persone raccoglie informazioni e potrà utilizzare tali conoscenze per stabilire che cosa è probabile che il pubblico in questione comprenda. Ad esempio, il titolare che raccoglie dati personali di professionisti potrà immaginare che il suo pubblico presenti un livello di comprensione superiore rispetto a quello cui si rivolge il titolare che ottiene dati personali di minori. Se non è certo del livello di intelligibilità e trasparenza delle informazioni e dell'efficacia delle interfacce utente/informative/dichiarazioni, ecc., il titolare può effettuare dei test, ad esempio ricorrendo, secondo il caso, a meccanismi quali gruppi di utenti, test di leggibilità, interazioni formali e informali e dialoghi con gruppi di settore, associazioni dei consumatori ed enti normativi.».

- **eventuali trasferimenti di dati in paesi terzi** (art.10 c. 2 lett. c d. lgs. 51/2018), che in questo caso non ve ne sono.

Le informative relative ai trattamenti con finalità di polizia, nelle copie fornite dal titolare del trattamento, **risultano conformi alla normativa vigente** (art. 10 c. 1 d. lgs. 51/2018).

B3.2.7 ACQUISIZIONE DEL CONSENSO DEGLI INTERESSATI (RISCHIO §37)

La necessità del consenso degli interessati (DS) al trattamento dei dati personali svolto dal Comune di Santeramo in Colle attraverso i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale è in funzione delle finalità perseguite, che in questo caso sono:

- **prevenzione, indagine, accertamento e perseguimento di reati, attività ausiliaria di salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 5 l. 65/1986 e art. 57 c.p.p.), con particolare riferimento alla sicurezza urbana (l. 48/2017)**, il consenso degli interessati per questa finalità non è richiesto, essendo funzioni escluse dall'applicazione del GDPR (art. 2 p. 2 lett. d GDPR) e per le quali la base giuridica lo esclude (art. 5 c. 1 d.lgs. 51/2018 e art. 5 l. 65/1986)....

Nel trattamento oggetto della presente valutazione non sono state violate le norme sul consenso degli interessati al trattamento dei propri dati personali.

B3.2.8 ESERCIZIO DEI DIRITTI DEGLI INTERESSATI E DIRITTO ALL'OBLIO (RISCHIO §38)

L'interessato al trattamento (DS) ha i seguenti diritti riconosciuti dalla normativa vigente:

a) **diritto di accesso** (art. 15 p. 1 lett. a-g GDPR e art. 11 c. 1 d. lgs. 51/2018), l'interessato ha il diritto di sapere dal titolare, senza ritardo, dell'esistenza di un trattamento dei propri dati personali e di avere accesso alle seguenti informazioni in tutti i casi:
   - le finalità e il titolo giuridico del trattamento;
   - le categorie di dati personali trattati;
   - i destinatari o le categorie di destinatari a cui i dati personali sono stati comunicati;
   - il periodo di conservazione dei dati personali o, se non è possibile, i criteri per determinare tale periodo;
   - tutte le informazioni disponibili sulla loro origine.
   - il diritto a essere informato che può chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano;
   - il diritto di proporre reclamo all'Autorità Garante, con i relativi dati di contatto;

   inoltre, quando la finalità del trattamento non sia la prevenzione, l'accertamento e la repressione dei reati e delle minacce alla pubblica sicurezza, il titolare ha il diritto di accesso anche a:
   - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, dando informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato (art. 15 p. 1 lett. h GDPR);
   - l'esistenza di garanzie adeguate (art. 46 GDPR) in caso di trasferimento dei dati in paesi terzi (art. 15 p. 2 GDPR).

b) **diritto di rettifica, cancellazione e limitazione di utilizzo**, (art. 16 GDPR e art. 12 d. lgs. 51/2018), l'interessato ha il diritto di ottenere dal titolare, senza ritardo, le seguenti azioni sui propri dati personali:
   - la rettifica dei dati personali che lo riguardano e che siano inesatti;
   - l'integrazione dei dati personali oggetto del trattamento che risultino incompleti;
   - la cancellazione dei dati personali che siano trattati illecitamente (art. 17 p. 1 lett. d), ovvero, nel caso di trattamenti finalizzati alla prevenzione, l'accertamento e la repressione dei reati e delle minacce alla pubblica sicurezza che violino specificatamente i principi applicabili al trattamento (art. 3 d. lgs. 51/2018), che non siano supportati da necessità specifica e idonee garanzie nel caso fossero categorie particolari di dati (art. 7 d. lgs. 51/2018) o che siano utilizzati in violazione di norme, qualora non possa essere immediatamente accertata l'esattezza dei dati ovvero essi servano per finalità probatorie il titolare può limitarne l'utilizzo anziché cancellarli;

c) **diritto all'oblio** (art. 16 GDPR e art. 12 d. lgs. 51/2018), nei casi in cui la finalità del trattamento non sia la prevenzione, l'accertamento e la repressione dei reati e delle minacce alla pubblica sicurezza, l'interessato può chiedere la cancellazione e il titolare del trattamento deve procedere, anche d'iniziativa senza che vi sia alcuna richiesta, a eliminare senza ritardo i dati personali quando (art.17 GDPR[153]).:
   - non siano più necessari rispetto alle finalità per le quali sono stati raccolti o comunque trattati (art. 17 p. 1 lett. a GDPR);
   - sia revocato il consenso al trattamento, quando ciò ne costituisca la base giuridica (art. 17 p. 1 lett. b GDPR).

L'interessato ha il diritto di ottenere dal titolare la sospensione del trattamento quando si contesti l'esattezza dei dati personali, il trattamento sia illecito e l'interessato si opponga alla cancellazione chiedendo che ne sia limitato l'utilizzo, i dati siano necessari all'interessato per fini giudiziari benché il titolare non ne abbia più bisogno ovvero il titolare si sia opposto al diritto di cancellazione nelle more della verifica dei motivi.

In questi casi i dati personali sono "contrassegnati" e trattati solo per la conservazione e, con il consenso dell'interessato, per le verifiche e le azioni di tutela dei diritti, allorquando venga meno la limitazione di utilizzo il titolare ha l'obbligo di avvisare l'interessato (art.18 GDPR[154]).

Nel trattamento oggetto della presente valutazione d'impatto, i diritti degli interessati riepilogati sopra **non sono esplicati ed esercitabili in maniera semplice** e accessibile per tutti. Il diritto all'oblio si realizza automaticamente al superamento del termine di ritenzione delle immagini che è di 7 giorni,

[153] Reg. (UE) UE 2016/679 GDPR, art. 17 :«*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: [...]*».

[154] Reg. (UE) UE 2016/679 GDPR, art. 18 (Diritto di limitazione del trattamento): «*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.*».

come si è indicato in precedenza, decorsi i quali le immagini registrate sono automaticamente sovrascritte dalle nuove.

B3.2.9 DEFINIZIONE DEGLI OBBLIGHI PER EVENTUALI RESPONSABILI DEL TRATTAMENTO (RISCHIO §39)

Nel caso oggetto della presente valutazione d'impatto-DPIA **manca l'accordo (DPA) tra titolare e responsabile del trattamento**, come si è già rilevato ed evidenziato in precedenza, quindi mancano le basi per poter valutare l'adeguata definizione degli obblighi per i soggetti responsabile del trattamento (DP).

B3.2.10 PROTEZIONE DEI DATI IN CASO DI TRASFERIMENTO IN PAESI TERZI (RISCHIO §40)

Non sono eseguiti trasferimenti di dati personali in paesi terzi.

B3.3 Criticità della sezione 3 e quantificazione del rischio

Segnalazione delle postazioni di ripresa (rischio §31)

Alcune aree sottoposte a videosorveglianza mancano delle tabelle informative e ciò può avere conseguenze gravi per le libertà e i diritti dei cittadini.

CALCOLO DEL RISCHIO §31	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	1,00

Contenuto delle informative di primo livello (rischio §32)

Il contenuto delle tabelle informative risulta completo di tutte le informazioni richieste dalla normativa (Linee guida 3/2019), quindi non si rilevano particolari rischi.

CALCOLO DEL RISCHIO §32	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Caratteristiche tecniche e posizionamento delle tabelle informative (rischio §33)

Le tabelle informative sono di dimensione non adeguate rispetto la posizione, l'altezza dal suolo e la distanza dal potenziale interessato oggetto di ripresa, con gravi conseguenze sulle sue libertà e i suoi diritti, con conseguenti rischi sui diritti e le libertà degli interessati.

CALCOLO DEL RISCHIO §33	Indice potenziale di magnitudo	0,50	Indice stimato di pericolo	0,50

Disponibilità delle informative di secondo livello (rischio §34)

Le informative di secondo livello risultano poco visibili e non adeguatamente complete e stratificate secondo le norme vigenti (Linee guida trasparenza e Linee guida videosorveglianza) e ciò costituisce un rischio rilevante per i diritti e le libertà degli interessati.

CALCOLO DEL RISCHIO §34	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	1,00

Contenuto delle informative di secondo livello (rischio §35)

Le copie fornite dal titolare risultano conformi alla normativa vigente (art. 13 e 14 GDPR).

CALCOLO DEL RISCHIO §35	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Contenuto delle informative per i trattamenti di polizia (rischio §36)

Le informative relative ai trattamenti con finalità di polizia risultano conformi alla normativa vigente (art. 10 c. 1 d. lgs. 51/2018) e quindi non si rilevano rischi.

CALCOLO DEL RISCHIO §36	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Acquisizione del consenso degli interessati (rischio §37)

Non si rilevano violazioni agli obblighi normativi e, di conseguenza, rischi per i diritti e le libertà degli interessati.

CALCOLO DEL RISCHIO §37	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Esercizio dei diritti degli interessati e diritto all'oblio (rischio §38)

I diritti degli interessati non sono esplicati in maniera chiara e intellegibile per tutti e non sono esercitabili in maniera semplice e accessibile per tutti e ciò costituisce un rischio rilevante per i diritti e le libertà degli interessati. Il diritto all'oblio si realizza automaticamente entro i termini di cancellazione delle immagini registrate che è stato indicato in precedenza.

CALCOLO DEL RISCHIO §38	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	0,50

Definizione degli obblighi per eventuali responsabili del trattamento (rischio §39)

Manca l'accordo tra titolare e responsabile del trattamento, già rilevato come precedente fattore di rischio, quindi non si può valutare l'adeguata definizione degli obblighi per il responsabile del trattamento.

CALCOLO DEL RISCHIO §39	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Protezione dei dati in caso di trasferimento in paesi terzi (rischio §40)

Non sono eseguiti trasferimenti di dati personali in paesi terzi.

CALCOLO DEL RISCHIO §40	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

B3.4 Piano di riduzione del rischio della sezione 3

Per ridurre il rischio del nuovo trattamento di cui alla presente valutazione d'impatto-DPIA, si segnala al titolare del trattamento e al RPD/DPO l'opportunità di rimediare in tempi brevi, nel rispetto dei principi di accountability (art. 24 GDPR) e di legalità e correttezza dei trattamenti per finalità di polizia (art. 15 d. lgs. 51/2018), alle criticità evidenziate nel paragrafo precedente.

Fermo restando la piena autonomia del titolare, si suggeriscono alcune attività che potrebbero essere adottate in tempi brevi e da verificare entro la prossima revisione della presente valutazione-DPIA, fissata fra 180 giorni ossia entro il 3/2/2027.

Sezione B3-Valutazione della necessità, proporzionalità e legittimità		**Risk mitigation**
RISCHIO	**MISURE DI MITIGAZIONE DEL RISCHIO**	
§31	*verifica della corretta apposizione delle tabelle informative prima dell'accesso in tutte le aree videosorvegliate;*	
§32	*nessuna necessaria.*	
§33	*verificare e adeguare le dimensione, la posizione, l'altezza dal suolo o la distanza dal potenziale interessato oggetto di ripresa in modo delle tabelle informative;*	
§34	*rendere facilmente accessibili le informative complete, in particolare sulla home page;*	
§35	*nessuna necessaria;*	
§36	*nessuna necessaria;*	
§37	*nessuna necessaria;*	
§38	*rendere più chiari e accessibili i diritti e le modalità di esercizio anche mettendo a disposizione degli interessati un modulo predefinito;*	
§39	*nessuna necessaria;*	
§40	*nessuna necessaria.*	
Indice di vulnerabilità stimato (Vu§3): 0,25-adeguate		

B3.5 Calcolo del rischio finale della sezione 3

Il rischio complessivo, con le procedure e i riferimenti indicati in precedenza, in attesa di ulteriore verifica alla prossima valutazione d'impatto, che consenta di stimare la vulnerabilità del sistema durante il funzionamento, all'esito dell'applicazione delle misure proposte per la riduzione del rischio e delle ulteriori che saranno adottate di propria iniziativa dal titolare, anche sulla base di eventuali indicazioni del responsabile per la protezione dei dati personali (RPD/DPO), risulta come segue:

Sezione B3-Valutazione della necessità, proporzionalità e legittimità				**Risk evaluation**
RISCHIO	**ELEMENTO VALUTATO**	**MAGNITUDO**	**PERICOLO**	
§31	Segnalazione delle postazioni di ripresa	1,00	1,00	
§32	Contenuto delle informative di primo livello	0,00	//	
§33	Caratteristiche tecniche e posizionamento delle tabelle informative	0,50	0,50	
§34	Disponibilità delle informative di secondo livello	1,00	1,00	
§35	Contenuto delle informative di secondo livello	0,00	//	
§36	Contenuto delle informative per finalità di polizia	0,00	//	
§37	Acquisizione del consenso degli interessati	0,00	//	
§38	Esercizio dei diritti degli interessati e diritto all'oblio	1,00	1,00	
§39	Definizione degli obblighi per eventuali responsabili del trattamento	0,00	//	
§40	Protezione dei dati in caso di trasferimento in paesi terzi	0,00	//	
Rischio emergente della sezione (Re§3)		3,50(*)	3,00(*)	**10,50-rilevante**
Indice di vulnerabilità (Vu§3)	0,25	**Rischio residuo (Rr§3)**		**2,63-medio**
Parere del RPD/DPO:		*vedasi eventuale giudizio allegato.*		
Giudizio del titolare del trattamento (DC):		*vedasi giudizio finale.*		

(*) Il rischio è limitato al valore massimo di 5 sia per la magnitudo e sia per il pericolo.

Sezione B4-Valutazione della sicurezza del sistema

B4.1 Premessa sulla valutazione del sistema

B4.1.1 LA NECESSITÀ DEL RISK ANALYSIS APPLICATO AL SISTEMA TECNOLOGICO

La vigente normativa europea richiede di valutare nel dettaglio la sicurezza del trattamento e quindi degli strumenti, delle interconnessioni, degli archivi utilizzati per il trattamento dei dati, sul piano fisico e logico, le misure di sicurezza e i meccanismi previsti per gestire e mitigare i rischi sulla sicurezza dei dati personali.

In questa sezione si analizzeranno i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale strumenti, i sistemi di archiviazione e le connessioni telematiche, le misure di sicurezza e i meccanismi adottati nel sistema oggetto della presente valutazione per garantire la protezione dei dati personali e il rispetto delle norme (art. 35 c.7 lett. d GDPR[155] e art. 23 c. 2 d. lgs. 51/2018).

B4.1.2 ELENCAZIONE DEI SISTEMI OGGETTO DELLA VALUTAZIONE

Il sistema di videosorveglianza valutato archivia le immagini su 1 pc server windows, 1 Dahua NVR608-64-4KS2, 1 Hikvision DS-7732NI-I4/16P(B) e dispone di 54 strumenti di ripresa complessivi, tutte di tipo IP ossia con gestione dell'immagine nativamente digitale e conseguente trasmissione digitale dei dati, ripartiti come segue:

Telecamere fisse: 50

- telecamere di contesto fisse: 24;
- telecamere di osservazione orientabili: 21;
- telecamere di rilevamento veicoli: 1;
- telecamere su barriere AP/ZTL: 4.

Telecamere mobili: 4

- telecamere mobili occultabili/fototrappole: 4;
- telecamere su veicoli/dashcam: //;
- sistemi mobili di sanzionamento con ripresa visiva: //;
- **telecamere indossabili/bodycam: 0;**
- **sistemi di ripresa aerea/droni: 0.**

Sistemi di radiolocalizzazione: 0

[155] Reg. (UE) 2016/679 GDPR, art.35: «*7. La valutazione contiene almeno:[...] d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*».

B4.1.3 ELEMENTI VALUTATI IN QUESTA SEZIONE

1) **sistema di archiviazione e di trasmissione delle immagini;**
2) **telecamere di contesto fisse;**
3) **telecamere d'osservazione orientabili;**
4) **telecamere di rilevamento veicoli e riconoscimento targhe;**
5) **sistemi di rilevamento transiti in AP/ZTL;**
6) **telecamere mobili occultabili/fototrappole;**
7) **telecamere installabili sui veicoli/dashcam;**
8) **sistemi di sanzionamento mobili basati su telecamere;**
9) **telecamere indossabili/bodycam;**
10) **sistema di ripresa aerea/droni.**

B4.2 Valutazione dei sistemi di gestione dei dati

B4.2.1 SISTEMA DI ARCHIVIAZIONE E TRASMISSIONE DELLE IMMAGINI (RISCHIO §41)

L'archiviazione delle immagini registrate dai mezzi di ripresa oggetto della presente valutazione avviene su **1 pc server windows, 1 Dahua NVR608-64-4KS2, 1 Hikvision DS-7732NI-I4/16P(B)**, con le caratteristiche tecniche riportate nella relazione tecnica allegata (-allegato 1-).

Il sistema deve garantire il rispetto delle norme sulla protezione dei dati e quindi la sicurezza del trattamento, attraverso l'adozione di idonee misure organizzative e tecniche adeguate per dimostrare l'accountability del titolare del trattamento (art. 24 c. 1 GDPR e art. 25 c. 1 d. lgs. 51/2018).

Il sistema di archiviazione delle immagini costituisce il cuore nevralgico del sistema poiché gestisce, archivia e rende disponibili i dati personali delle persone riprese e quindi deve essere protetto sia durante la fase dinamica dei trasferimenti dei dati (acquisizione e riproduzione) e sia durante la fase statica dell'archiviazione.

La valutazione del sistema di archiviazione si è svolta sui seguenti piani:

a) **sicurezza fisica** (Linee guida videosorveglianza punto 9.3.2-132 p. 35), valutando la protezione e resilienza in caso di interferenze volontarie e involontarie sulla parte hardware e quindi sulle macchine elettroniche, quindi la protezione da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e danni accidentali, come ad esempio, sovratensioni elettriche, temperature estreme e riversamento di caffè;

b) **sicurezza del sistema e dei dati** (Linee guida videosorveglianza punto 9.3.2-134 p. 35), valutando la protezione e resilienza sulla parte software e quindi del contenuto informatico in caso di interferenze volontarie e involontarie nel suo normale funzionamento quindi la protezione accesso abusivo al sistema, sottrazione, utilizzo abusivo, danneggiamento, alterazione, blocco del sistema, come ad esempio virus, malaware, spyware, ransomware, accessi abusivi al sistema informatico;

c) **il controllo degli accessi** (Linee guida videosorveglianza punto 9.3.2-135 p. 35-36), valutando i sistemi e le procedure per garantire che solo le persone autorizzate possano accedere al sistema e ai dati, impedendo a chiunque altro di farlo.

Concretamente alcune misure organizzative e di sicurezza sono esplicitamente consigliate (Linee guida videosorveglianza 9.3.1 e 9.3.2) e sono addirittura obbligatorie nel caso di trattamenti

finalizzati alla prevenzione, accertamento e repressione di reati e minacce alla sicurezza pubblica (art. 25 c. 2 d. lgs. 51/2018), come sono svolti dal sistema oggetto della presente valutazione d'impatto.

Quindi nella valutazione della sicurezza del sistema di archiviazione delle immagini si terrà conto del:

a) **controllo dell'accesso fisico**, verificando che non ci sia il rischio di accessi non autorizzati ai locali di archiviazione delle immagini, ricorrendo all'archiviazione in cloud oppure installando i sistemi di archiviazione in locali chiusi e possibilmente presidiati che abbiano livelli di sicurezza idonea con:
   - porta blindata possibilmente controllata da chiave elettronica;
   - grate alle eventuali finestre che non siano inaccessibili per altezza dal suolo;
   - climatizzazione per evitare il surriscaldamento dei dispositivi elettronici;
   - sistema antincendio.

b) **controllo della sicurezza dei dati archiviati**, verificando che non ci sia il rischio di accessi non autorizzati ai dati archiviati e che:
   - i monitor siano orientati in maniera da non permettere la visualizzazione ad altri soggetti estranei;
   - laddove l'archiviazione non sia in cloud siano presenti idonei sistemi firewall e antivirus/antimalaware aggiornati.

c) **controllo degli accessi logici**, verificando che non ci si il rischio di accessi non autorizzati al sistema di videosorveglianza e che:
   - ogni utente disponga di una password univoca che rispetti i requisiti di sicurezza;
   - ogni utenza consenta l'accesso personalizzato solo ai dati e alle parti autorizzate.

d) **verifica file log degli utenti**, per poter verificare e accertare a posteriori:
   - chi abbia avuto accesso al sistema;
   - quali dati personali siano stati gestiti nell'archivio;
   - la cronodatazione di ogni accesso.

e) **controllo della ridondanza**, per garantire che i sistemi di archiviazione e i dati in essi contenuti possano essere ripristinati in caso di perdita;

f) **controllo dell'affidabilità e integrità del sistema**, per garantire che le funzioni del sistema siano sempre operative e che eventuali errori di funzionamento siano segnalati (affidabilità) e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema (integrità).

A) Valutazione del sistema di trasmissione delle immagini

I punti di ripesa sono interconnessi al sistema centrale di registrazione con un sistema telematico che mette in connessione i punti di ripresa con il sistema di archiviazione dei dati e, quindi, di visualizzazione delle immagini prevede rete mista cavo e radio punto-punto con trasmissione dati cifrati..

Il controllo degli accessi per la visualizzazione in tempo reale è consentito solo facendo il login sul server, non si è verificato il sistema di gestione delle password, ma si raccomanda di fare riferimento, per quanto applicabile a sistemi non SPID, alle regole generali del LoA2 dell'ISO-IEC29115, a cui fa riferimento la normativa AGID, utilizzando i seguenti accorgimenti:

- lunghezza minima di otto caratteri;
- uso di caratteri maiuscoli e minuscoli;
- inclusione di uno o più caratteri numerici;
- non deve contenere più di due caratteri identici consecutivi;
- inclusione di almeno un carattere speciali ad es #, $,% ecc;
- validità non superiore a 180 giorni.

Il controllo dell'accesso ai dati registrati è realizzato mediante la crittografia dei dati che consente solo ai soggetti in possesso della chiave autorizzati di avere, mediante la chiave di crittografia, l'accesso alle immagini fotografiche e ai filmati audiovisivi, pertanto non si rilevano particolari criticità.

B) Valutazione del sistema di archiviazione delle immagini

Sulla base degli elementi e criteri indicati in precedenza non sono state rilevate criticità e nei successivi aggiornamenti, che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione.

B4.3 Valutazione dei sistemi ripresa fissi

B4.3.1 TELECAMERE DI CONTESTO FISSE (RISCHIO §42)

Le telecamere di contesto sono sistemi che non consentono di variare la zona inquadrata se non eventualmente, per modificare il fattore di ingrandimento e quindi l'angolo di ripresa attraverso sistemi di zoom digitali o analogici.

Nel sistema oggetto della presente valutazione sono presenti **n. 14 Dahua IPC-HFW8301EN, n. 4 Dahua IPC-HFW3441T-ZAS/ZS-S2, n. 4 Hikvision DS-2CD6D55G2-IZHS/NFC, n. 2 Elmo PROIBF02D**, con le caratteristiche riportate nella relazione tecnica allegata (-allegato 1-).

La valutazione della sicurezza di questo sistema di acquisizione dei dati si è svolta sui seguenti punti (Linee guida videosorveglianza):

-**protezione dei dati**, attraverso l'archiviazione remota delle immagini ovvero l'implementazione di sistemi di crittografia;

-**sicurezza dell'installazione**, per posizione e altezza da terra come misura di protezione da tentativi di sottrazione o danneggiamento;

-**protezione della telecamera**, dagli agenti atmosferici, dalla polvere e dagli impatti di eventuali colpi con corpi contundenti per finalità illecite;

-**sicurezza informatica**, attraverso sistemi di cybersicurezza che proteggano l'accesso remoto non autorizzato ai dispositivi di ripresa e al sistema di trasmissione delle immagini.

Sulla base degli elementi e criteri indicati in precedenza non sono state rilevate criticità e nei successivi aggiornamenti, che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione.

B4.3.2 TELECAMERE D'OSSERVAZIONE ORIENTABILI (RISCHIO §43)

Le telecamere di osservazione sono sistemi di ripresa dotate della capacità di brandeggio dell'obiettivo, in modo da assicurare la visione completa a 360° sul piano orizzontale e a circa 180° sul piano verticale o comunque per buona parte di queste aree.

Nel sistema oggetto della presente valutazione sono presenti **n. 20 Dahua SD6C230S-HN, n. 1 RaySharp/Zhuhai RS-CH848M6CC37-HLA-A**, con le caratteristiche riportate nella relazione tecnica allegata (-allegato 1-).

La valutazione della sicurezza di questo sistema di acquisizione dei dati si è svolta sui seguenti punti (Linee guida videosorveglianza):

-**protezione dei dati**, attraverso l'archiviazione remota delle immagini ovvero l'implementazione di sistemi di crittografia;

-**sicurezza dell'installazione**, per posizione e altezza da terra come misura di protezione da tentativi di sottrazione o danneggiamento;

-**protezione della telecamera**, dagli agenti atmosferici, dalla polvere e dagli impatti di eventuali colpi con corpi contundenti per finalità illecite;

-**sicurezza informatica**, attraverso sistemi di cybersicurezza che proteggano l'accesso remoto non autorizzato ai dispositivi di ripresa e al sistema di trasmissione delle immagini.

Sulla base degli elementi e criteri indicati in precedenza, non sono state rilevate criticità e, nei successivi aggiornamenti che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione.

B4.3.3 TELECAMERE DI RILEVAMENTO VEICOLI E LETTURA TARGHE (RISCHIO §44)

Le telecamere con capacità di rilevazione transiti e lettura targhe, note anche con l'acronimo anglosassone LPR (*License Plate Recognition=riconoscimento targhe*) o ANPR (*Automatic Number Plate Recognition=riconoscimento automatico del numero di targa*), sono sistemi audiovisivi che consentono di rilevare il transito dei veicoli anche a rilevante velocità e in condizione di scarsa illuminazione e, integrando onboard un sistema di riconoscimento caratteri, anche di leggere e memorizzare le targhe applicate agli autoveicoli e ai motoveicoli.

Questi sistemi possono limitarsi a registrare i dati del veicolo ai fini di prevenzione e repressione dei crimini, ad esempio collegandosi alla banca dati dei veicoli rubati per inviare degli allarmi alle forze di polizia, ovvero poter abbinare altri sensori e tecnologie per rilevare e documentare violazioni alle norme amministrative, come ad esempio l'eccesso di velocità, il passaggio con il semaforo rosso, il transito su corsie riservate, la mancanza della copertura assicurativa o l'omissione della revisione.

Nel sistema oggetto della presente valutazione è presente **n. 1 Elmo ANPR2MPX**, con le caratteristiche riportate nella relazione tecnica allegata (-allegato 1-).

La valutazione della sicurezza di questo sistema di acquisizione dei dati si è svolta sui seguenti punti (Linee guida videosorveglianza):

-**protezione dei dati**, attraverso l'archiviazione remota delle immagini ovvero l'implementazione di sistemi di crittografia;

-**sicurezza dell'installazione**, per posizione e altezza da terra come misura di protezione da tentativi di sottrazione o danneggiamento;

-**protezione della telecamera**, dagli agenti atmosferici, dalla polvere e dagli impatti di eventuali colpi con corpi contundenti per finalità illecite;

-**sicurezza informatica**, attraverso sistemi di cybersicurezza che proteggano l'accesso remoto non autorizzato ai dispositivi di ripresa e al sistema di trasmissione delle immagini.

Sulla base degli elementi e criteri indicati in precedenza, non sono state rilevate criticità e, nei successivi aggiornamenti che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione.

B4.3.4 SISTEMI DI RILEVAMENTO TRANSITI IN AP/ZTL (RISCHIO §45)

Questi sistemi posti su barriere in prossimità degli accessi alle zone a traffico limitato (acronimo ZTL) o alle aree pedonali (acronimo AP), integrano generalmente telecamere di contesto con altre di rilevamento veicoli e, attraverso la comparazione nella banca dati (white list/black list) rilevano i veicoli non autorizzati al transito per il successivo sanzionamento ai sensi della vigente normativa del Codice della Strada.

Nel sistema oggetto della presente valutazione sono presenti **n. 4 Project Automation K53700-R2/K53700-02**, con le caratteristiche riportate nella relazione tecnica allegata (-allegato 1-).

La valutazione della sicurezza di questo sistema di acquisizione dei dati si è svolta sui seguenti punti (Linee guida videosorveglianza):

-**protezione dei dati**, attraverso l'archiviazione remota delle immagini ovvero l'implementazione di sistemi di crittografia;

-**sicurezza dell'installazione**, per posizione e altezza da terra come misura di protezione da tentativi di sottrazione o danneggiamento;

-**protezione della telecamera**, dagli agenti atmosferici, dalla polvere e dagli impatti di eventuali colpi con corpi contundenti per finalità illecite;

-**sicurezza informatica**, attraverso sistemi di cybersicurezza che proteggano l'accesso remoto non autorizzato ai dispositivi di ripresa e al sistema di trasmissione delle immagini.

Sulla base degli elementi e criteri indicati in precedenza non sono state rilevate criticità e nei successivi aggiornamenti, che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione.

B4.4 Valutazione dei sistemi di rilevamento mobili

B4.4.1 TELECAMERE MOBILI OCCULTABILI/FOTOTRAPPOLE (RISCHIO §46)

Le fototrappole sono sistemi mobili di videosorveglianza posizionati in maniera poco visibile allo scopo di documentare comportamenti illeciti e identificarne i responsabili.

Le fototrappole si compongono di una telecamera autoalimentata con accumulatori (batterie alcaline o ricaricabili), di norma equipaggiate con illuminatore all'infrarosso che permette di riprendere immagini anche di notte, unita a un sensore che attiva la ripresa appena rileva un movimento o altro stimolo, come ad esempio un suono o una variazione termica che evidenzi una presenza di esseri animati, ottimizzando in questo modo la memoria e la durata della batteria.

La memorizzazione delle immagini può avvenire in locale, ma in questi casi si deve avere un sistema di criptazione dei dati di livello tale da escludere rischi di accesso abusivo ai dati, oppure possono avere sistemi di trasmissione dati via wi-fi ovvero via rete dati cellulare GSM/UMTS.

Sono presenti **n. 4 Reolink Go Ranger PT 4K**, con le caratteristiche riportate nella relazione tecnica allegata (-allegato 1-).

La valutazione della sicurezza di questo sistema di acquisizione dei dati si è svolta sui seguenti punti (Linee guida videosorveglianza):

-**protezione dei dati**, attraverso l'archiviazione remota delle immagini ovvero l'implementazione di sistemi di crittografia;

-**protezione antifurto**, attraverso idonei sistemi fisici, di segnalazione e localizzazione remota dello spostamento non autorizzato per impedire rischi di accesso illecito e sottrazione dei dati;

-**protezione della telecamera**, dagli agenti atmosferici, dalla polvere e dagli impatti di eventuali colpi con corpi contundenti per finalità illecite;

-**sicurezza informatica**, attraverso sistemi di cybersicurezza che proteggano l'accesso remoto non autorizzato ai dispositivi di ripresa e al sistema di trasmissione delle immagini.

Sulla base degli elementi e criteri indicati in precedenza sono state rilevate le seguenti criticità: sistema di ridondanza/backup, affidabilità e integrità del sistemain contrasto con le norme vigenti (Linee guida videosorveglianza 9.3.1 e 9.3.2 e art. 25 c. 2 d. lgs. 51/2018).

B4.4.2 TELECAMERE INSTALLABILI SU VEICOLI/DASHCAM (RISCHIO §47)

Le dashcam, abbreviazione di dashboard camera con il significato di telecamera da cruscotto, sono sistemi di ripresa installati all'interno dei veicoli, generalmente sul cruscotto o all'interno del parabrezza e comunque in posizione tale da non ostruire la visuale, allo scopo di registrare tutto quel che accade all'esterno durante la guida e la fermata.

Nel sistema oggetto della presente valutazione il titolare del trattamento ha dichiarato che non sono presenti telecamere installabili su veicoli/dashcam e quindi non si è valutata questa sezione.

B4.4.3 SISTEMI DI SANZIONAMENTO MOBILI BASATI SU TELECAMERE (RISCHIO §48)

I sistemi di sanzionamento mobile che utilizzano strumenti di ripresa visiva per rilevare e documentare violazioni alle norme amministrative, come ad esempio l'eccesso di velocità, il passaggio con il semaforo rosso, la sosta vietata, il transito su corsie riservate, la mancanza della copertura assicurativa o l'omissione della revisione. Non sono valutati in questa sezione i sistemi che svolgono queste funzioni in installazione fissa, poiché sono considerati nelle precedente sezione B4.3.3 telecamere di rilevamento veicoli e lettura targhe (rischio §44) a pag. 97.

Nel sistema oggetto della presente valutazione il titolare del trattamento ha dichiarato che non sono presenti sistemi di sanzionamento mobili che effettuino riprese di immagini fisse o in movimento e quindi non si è valutata questa sezione.

B4.4.4 TELECAMERE INDOSSABILI/BODYCAM (RISCHIO §49)

Questi sistemi di telecamere mobili sono indossate sul petto degli operatori per riprendere e documentare ciò ciò che accade nel loro campo visivo. Sono uno strumento particolarmente invasivo

per i diritti e le libertà dei cittadini e pertanto se ne deve valutare attentamente la necessità bilanciandone i diritti, così come si è già visto in precedenza[156].

Nel sistema oggetto della presente valutazione il titolare del trattamento ha dichiarato che non sono presenti telecamere indossabili/bodycam e quindi non si è valutata questa sezione.

B4.4.5 SISTEMI DI RIPRESA AEREA/DRONI (RISCHIO §50)

Sono velivoli, noti anche con l'acronimo UAV (unmanned aerial vehicle) o UAS (unmanned aerial system) o sistema aereo senza pilota, che consentono di effettuare riprese e altre operazioni dall'alto; sono considerati aeromobili a tutti gli effetti e, quindi, devono rispettare le stesse regole e le procedure degli aerei con pilota ed equipaggio a bordo.

Nel sistema oggetto della presente valutazione il titolare del trattamento ha dichiarato che non sono presenti sistemi di ripresa aerea/droni e quindi non si è valutata questa sezione.

B4.5 Criticità della sezione 4 e quantificazione del rischio

Sistema di archiviazione e trasmissione delle immagini (rischio §41)

Il sistema di archiviazione dei dati non evidenzia particolari criticità.

CALCOLO DEL RISCHIO §41	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Telecamere di contesto fisso (rischio §42)

Le telecamere di contesto non evidenziano particolari criticità.

CALCOLO DEL RISCHIO §42	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Telecamere di osservazione orientabili (rischio §43)

Le telecamere d'osservazione non evidenziano particolari criticità.

CALCOLO DEL RISCHIO §43	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Telecamere di rilevamento veicoli e lettura targhe (rischio §44)

Le telecamere di rilevamento veicoli non evidenziano particolari criticità.

CALCOLO DEL RISCHIO §44	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Sistemi di rilevamento transiti in AP/ZTL (rischio §45)

Le telecamere di rilevamento transiti nelle zone a traffico controllato (AP/ZTL) non evidenziano particolari criticità.

CALCOLO DEL RISCHIO §45	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

[156] Si veda il paragrafo B2.2.9 conformità dell'eventuale trattamento con bodycam (rischio §29) a pagina 80.

Telecamere mobili occultabili/fototrappole (rischio §46)

Le telecamere occultabili/fototrappole risultano carenti di sistema di ridondanza/backup, affidabilità e integrità del sistema ciò costituisce un rischio per la sicurezza dei dati trattati dal sistema.

CALCOLO DEL RISCHIO §46	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	0,50

Telecamere installabili sui veicoli/dashcam (rischio §47)

Non sono presenti telecamere installabili sui veicoli/dash cam.

CALCOLO DEL RISCHIO §47	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Sistemi di sanzionamento mobili basati su telecamere (rischio §48)

Non sono presenti sistemi mobili di sanzionamento.

CALCOLO DEL RISCHIO §48	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Telecamere indossabili/bodycam (rischio §49)

Non sono presenti telecamere indossabili/body cam.

CALCOLO DEL RISCHIO §49	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Sistemi di ripresa aerea/droni (rischio §50)

Non sono presenti sistemi di ripresa aerea/droni.

CALCOLO DEL RISCHIO §50	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

B4.6 Piano di riduzione del rischio della sezione 4

Per ridurre il rischio del nuovo trattamento di cui alla presente valutazione d'impatto-DPIA, si segnala al titolare del trattamento e al RPD/DPO l'opportunità di rimediare in tempi brevi, nel rispetto dei principi di accountability (art. 24 GDPR) e di legalità e correttezza dei trattamenti per finalità di polizia (art. 15 d. lgs. 51/2018), alle criticità evidenziate nel paragrafo precedente.

Fermo restando la piena autonomia del titolare, si suggeriscono alcune attività che potrebbero essere adottate in tempi brevi e da verificare entro la prossima revisione della presente valutazione-DPIA, fissata fra 180 giorni ossia entro il 3/2/2027.

Sezione B4-Valutazione della sicurezza del sistema		**Risk mitigation**
RISCHIO	**MISURE DI MITIGAZIONE DEL RISCHIO**	
§41	*nessuna necessaria;*	
§42	*nessuna necessaria;*	
§43	*nessuna necessaria;*	
§44	*nessuna necessaria;*	
§45	*nessuna necessaria;*	
§46	*adeguare sistema di ridondanza/backup, affidabilità e integrità del sistema come previsto dalle norme vigenti ovvero sostituirle;*	
§47	//	
§48	//	
§49	//	
§50	//	
Indice di vulnerabilità stimato (Vu§4): 0,50-parzialmente adeguate o da verificare		

B4.7 Calcolo del rischio finale della sezione 4

Il rischio complessivo, con le procedure e i riferimenti indicati in precedenza, in attesa di ulteriore verifica alla prossima valutazione d'impatto, che consenta di stimare la vulnerabilità del sistema durante il funzionamento, all'esito dell'applicazione delle misure proposte per la riduzione del rischio e delle ulteriori che saranno adottate di propria iniziativa dal titolare, anche sulla base di eventuali indicazioni del responsabile per la protezione dei dati personali (RPD/DPO), risulta come segue:

Sezione B4-Valutazione della sicurezza del sistema				**Risk evaluation**
RISCHIO	**ELEMENTO VALUTATO**	**MAGNITUDO**	**PERICOLO**	
§41	Sistema di archiviazione e trasmissione delle immagini	0,00	//	
§42	Telecamere di contesto fisso	0,00	//	
§43	Telecamere di osservazione orientabili	0,00	//	
§44	Telecamere di rilevamento veicoli e lettura targhe	0,00	//	
§45	Sistemi di rilevamento transiti in AP/ZTL	0,00	//	
§46	Telecamere mobili occultabili/fototrappole	1,00	0,50	
§47	Telecamere installabili sui veicoli/dashcam	n.d.	//	
§48	Sistemi di sanzionamento mobili basati su telecamere	n.d.	//	
§49	Telecamere indossabili/bodycam	n.d.	//	
§50	Sistemi di ripresa aerea/droni	0,00	//	
Rischio emergente della sezione (Re§4)		1,00(*)	0,50(*)	**0,50-basso**
Indice di vulnerabilità (Vu§4)	0,50	**Rischio residuo (Rr§4)**		**0,25-basso**
Parere del RPD/DPO:		*vedasi eventuale giudizio allegato.*		
Giudizio del titolare del trattamento (DC):		*vedasi giudizio finale.*		

(*) Il rischio è limitato al valore massimo di 5 sia per la magnitudo e sia per il pericolo.

Sezione B5-Valutazione del posizionamento dei sistemi di ripresa

B5.1 Premessa sulla valutazione del posizionamento dei sistemi di ripresa

B5.1.1 OBBLIGO DI VALUTAZIONE

Il GDPR impone di valutare i rischi sulle libertà democratiche e sui diritti dei cittadini derivanti dal trattamento dei dati, in particolar modo nel caso dei sistemi di videosorveglianza per i quali è sempre obbligatoria la valutazione d'impatto-DPIA, e di predisporre le misure più efficaci in modo da poter dimostrare la conformità del trattamento alle precisioni del Regolamento Europeo (art.35 c.7 p.d GDPR), in questa parte si valuterà il posizionamento e le modalità di impiego operativo dell'impianto di videosorveglianza.

B5.1.2 SCOPO DELL'ANALISI DELLA PRESENTE SEZIONE

La videosorveglianza, comunque sia realizzata, dalle postazioni fisse a quelle mobili includendo anche quelle indossate dagli operatori, è consentito per la prevenzione e l'accertamento di illeciti a condizione che non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate[157].

Dopo aver verificato la legittimità e la sicurezza del trattamento, l'idoneità e l'affidabilità dei mezzi impiegati, l'analisi svolta in questa sezione ha lo scopo di verificare la diretta correlazione delle 54 telecamere che compongono il sistema con le finalità di finalità istituzionali dell'ente, compresa la polizia amministrativa, l'accertamento delle violazioni amministrative (art. 13 l.689/81) e l'attività di polizia stradale (art. 11 CdS), che sono dichiarate dal titolare del trattamento e che sono state verificate in precedenza.

L'analisi quindi valuta il posizionamento delle telecamere, il campo di inquadratura e il periodo di funzionamento esaminando i luoghi e i soggetti che possono essere effettivamente ripresi e, di conseguenza, i dati personali che possono essere trattati per verificare innanzitutto che non siano trattati e quindi ripresi categorie particolari di dati (art. 9 GDPR e art. 7 d. lgs. 51/2018), come ad esempio sedi di partito sindacati, centri sanitari che possano rivelare la patologia di cui soffre l'interessato al trattamento, locali e contesti che potrebbero indicare l'orientamento sessuale, ecc.

Nell'ottica dell'accountability, si verifica anche il rispetto del principio generale di minimizzazione dei dati e quindi l'effettiva necessità, proporzionalità e la diretta correlazione dei mezzi e dell'area ripresa con l'attività di polizia (art. 3 c.1 DPR 15/2018) per le specifiche finalità di prevenzione, indagine, accertamento e perseguimento di reati, attività ausiliaria di salvaguardia e prevenzione di minacce alla sicurezza pubblica (art. 5 l. 65/1986 e art. 57 c.p.p.), con particolare riferimento alla sicurezza urbana (l. 48/2017) con l'esigenza effettiva di assolvere le finalità di .

Nel caso dalle categorie particolari di dati, in particolare, si richiede come principio generale che i sistemi di videosorveglianza riducano al minimo o escludano del tutto, laddove possibile, la ripresa di immagini che possano rivelare categorie particolari di dati anche quando il loro trattamento è consentito (Linee guida videosorveglianza punto 5.66[158]).

---

[157] D.P.R. 15/2018, art. 3. (Finalità dei trattamenti): «*1. I trattamenti di dati personali si intendono effettuati per le finalità di polizia, ai sensi dell'articolo 53 del Codice, quando sono direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati.[...]*».

[158] European Data Protection Board, Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, punto 5.66 (Trattamenti riguardanti categorie particolari di dati): «*In via generale e in linea di principio, ogniqualvolta si installa un sistema di*

B5.1.3 ELEMENTI VALUTATI IN QUESTA SEZIONE

1) **posizionamento delle telecamere di contesto fisse;**
2) **posizionamento delle telecamere d'osservazione orientabili;**
3) **posizionamento delle telecamere rilevamento veicoli e lettura targhe;**
4) **posizionamento dei sistemi di rilevamento transiti in ZTL/AP;**
5) **impiego delle telecamere mobili occultabili/fototrappole;**
6) **impiego delle telecamere mobili installabili sui veicoli/dashcam;**
7) **impiego dei sistemi di sanzionamento mobili basati su telecamere;**
8) **impiego delle telecamere indossabili/bodycam;**
9) **impiego dei sistemi di ripresa aerea;**
10) **sistemi di localizzazione remota.**

B5.2 Valutazione del posizionamento degli strumenti di ripresa fissi

B5.2.1 MINIMIZZAZIONE DELLE POSTAZIONI INTERESSATE DALLA VIDEOSORVEGLIANZA FISSA

A. elencazione

Il sistema di videosorveglianza valutato nel presente documento prevede 50 telecamere fisse delle seguenti tipologie:

-telecamere di contesto fisse: 24;

-telecamere di osservazione orientabili: 21;

-telecamere di rilevamento veicoli: 1;

-telecamere su barriere ZTL/AP: 4.

B. criterio di valutazione

La valutazione della legittima collocazione si è svolta verificando che non siano inquadrati luoghi che possano rilevare dati personali rientranti nelle categorie particolari (art. 9 GDPR e art. 7 d. lgs. 51/2018), che devono sempre essere ridotte al minimo indispensabile ed escluso in tutti i casi possibili (Linee guida videosorveglianza punto 5.66) ovvero informazioni sottoposte a tutele particolari (art. 4 l. 300/1970), salvo che sussista una necessità essenziale per le finalità del trattamento in presenza di una specifica base giuridica che ne legittimi l'impiego, e quindi che non siano ripresi, in particolare:

-luoghi di lavoro, nelle aree in cui sia possibile sorvegliare a distanza i lavoratori da parte del datore di lavoro;

-sedi di partiti e movimenti politici, che possano consentire di rilevare dati sulle frequentazioni e sulle preferenze politiche, anche in via presuntiva, dei soggetti ripresi;

-sedi di strutture sindacali, che possano consentire di presumere appartenenze o simpatie sindacali;

---

videosorveglianza si dovrebbe prestare particolare attenzione al principio della minimizzazione dei dati. Pertanto, anche nei casi in cui l'articolo 9, paragrafo 1, non si applica, il titolare del trattamento dovrebbe sempre cercare di ridurre al minimo il rischio di acquisire filmati che rivelino altri dati sensibili (al di là dell'articolo 9), indipendentemente dalla finalità.».

-luoghi di culto, sedi di organizzazioni religiose o circoli filosofici, che permettano di rilevare le convinzioni religiose o filosofiche dei soggetti ripresi;

-sedi di associazioni lgbtqia+, di sexy shops o altri locali che possano rivelare, anche indirettamente, gli orientamenti sessuali dei soggetti inquadrati;

-scuole nel periodo in cui siano adibite a seggi elettorali e che possano quindi rilevare quali soggetti esercitino il diritto di voto e, in via induttiva e presuntiva, le idee politiche in funzione delle relazioni con eventuali candidati o rappresentanti di partiti e movimenti politici.

Non sono disponibili mappe, planimetrie ubicative o altri elaborati grafici.

Fermo restando la scadenza della presente valutazione alla data del 3/2/2027 e della conseguente necessità di aggiornamento, si consiglia di verificare periodicamente, con controlli a campione di spezzoni di registrazioni casuali, l'effettiva necessità delle telecamere e dell'area ripresa ai fini dell'attività di polizia e la natura e quantità dei dati registrati a intervalli di tempo oppure in sede di verifica a tempo.

B5.2.2 POSIZIONAMENTO DELLE TELECAMERE DI CONTESTO FISSE (RISCHIO 51)

Nel sistema valutato sono presenti **n. 14 Dahua IPC-HFW8301EN, n. 4 Dahua IPC-HFW3441T-ZAS/ZS-S2, n. 4 Hikvision DS-2CD6D55G2-IZHS/NFC, n. 2 Elmo PROIBF02D**, posizionate nei luoghi indicati nella relazione tecnica ubicativa allegata (-allegato 1-).

Sulla base degli elementi e criteri indicati in precedenza, si è rilevato che sono inquadrate aree e contesti che possono rivelare informazioni relative all'attività lavorativa dei dipendenti del titolare degli interessati e ciò costituisce un elemento di rischio da valutare attentamente sia per l'effettiva necessita e sia nel quantitativo di dati acquisiti e nel tempo del trattamento (Linee guida videosorveglianza 9.3.1 e 9.3.2 e art. 25 c. 2 d. lgs. 51/2018), aspetto superabile con la rimozione ovvero modifica del settore inquadrato

B5.2.3 POSIZIONAMENTO DELLE TELECAMERE D'OSSERVAZIONE ORIENTABILI (RISCHIO §52)

Nel sistema valutato sono presenti **n. 20 Dahua SD6C230S-HN, n. 1 RaySharp/Zhuhai RS-CH848M6CC37-HLA-A**, posizionate nei luoghi indicati nella relazione tecnica ubicativa allegata (-allegato 1-).

Sulla base degli elementi e criteri indicati in precedenza, si è rilevato che sono inquadrate aree e contesti che possono rivelare informazioni relative all'attività lavorativa dei dipendenti del titolare degli interessati e ciò costituisce un elemento di rischio da valutare attentamente sia per l'effettiva necessita e sia nel quantitativo di dati acquisiti e nel tempo del trattamento (Linee guida videosorveglianza 9.3.1 e 9.3.2 e art. 25 c. 2 d. lgs. 51/2018), aspetto superabile con la rimozione ovvero modifica del settore inquadrato

B5.2.4 POSIZIONAMENTO DELLE TELECAMERE RILEVAMENTO VEICOLI E LETTURA TARGHE (RISCHIO §53)

Nel sistema valutato è presente **n. 1 Elmo ANPR2MPX**, posizionata nel luogo indicato nella relazione tecnica ubicativa allegata (-allegato 1-).

Sulla base degli elementi e criteri indicati in precedenza, non sono state rilevate criticità e, nei successivi aggiornamenti, che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione

B5.2.5 POSIZIONAMENTO DEI SISTEMI DI RILEVAMENTO TRANSITI IN AP/ZTL (RISCHIO §54)

Nel sistema valutato sono presenti **n. 4 Project Automation K53700-R2/K53700-02**, posizionate nei luoghi indicati nella relazione tecnica ubicativa allegata (-allegato 1-).

Sulla base degli elementi e criteri indicati in precedenza, non sono state rilevate criticità e, nei successivi aggiornamenti, che saranno svolti alla scandenza della presente valutazione ovvero laddove altri elementi richiedessero una rivalutazione anticipata, si approfondirà e verificherà la sussistenza di questa condizione

B5.3 Valutazione del posizionamento degli strumenti di ripresa mobili

B5.3.1 MINIMIZZAZIONE DELLE POSTAZIONI INTERESSATE DALLA VIDEOSORVEGLIANZA MOBILE

A. elencazione

Il sistema di videosorveglianza valutato nel presente documento prevede 4 telecamere mobili delle seguenti tipologie:

-**fototrappole**: 4;

-**telecamere installabili sui veicoli/dashcam**: nessuna;

-**sistemi di sanzionamento mobili**: nessuno;

-**telecamere indossabili/bodycam**: nessuna.

B. criterio di valutazione

I sistemi mobili, per loro natura, non possono essere valutati nel loro posizionamento quindi si possono valutare nelle privacy policies definite per essi nelle Linee guida per la protezione dei dati personali e la disciplina tecnica e organizzativa dei trattamenti anche mediante il sistema di videosorveglianza, ai sensi dell'art. 24 par. 1 del GDPR e dell'art. 15 del d. lgs. 51/2018.

Tuttavia per valutare correttamente il rispetto delle norme in materia di protezione dei dati personali e, quindi, dei diritti e delle libertà fondamentali dei cittadini si dovrebbe disporre almeno di una zonizzazione generale ove si prevede di impiegare i sistemi di videosorveglianza mobile affinché si possa escludere che siano inquadrati luoghi che possano rilevare dati personali rientranti nelle categorie particolari (art. 9 GDPR e art. 7 d. lgs. 51/2018), che devono sempre essere ridotte al minimo indispensabile ed escluso in tutti i casi possibili (Linee guida videosorveglianza punto 5.66) ovvero informazioni sottoposte a tutele particolari (art. 4 l. 300/1970), salvo che sussista una necessità essenziale per le finalità del trattamento in presenza di una specifica base giuridica che ne legittimi l'impiego, e quindi che non siano ripresi, in particolare:

-luoghi di lavoro, nelle aree in cui sia possibile sorvegliare a distanza i lavoratori da parte del datore di lavoro;

-sedi di partiti e movimenti politici, che possano consentire di rilevare dati sulle frequentazioni e sulle preferenze politiche, anche in via presuntiva, dei soggetti ripresi;

-sedi di strutture sindacali, che possano consentire di presumere appartenenze o simpatie sindacali;

-luoghi di culto, sedi di organizzazioni religiose o circoli filosofici, che permettano di rilevare le convinzioni religiose o filosofiche dei soggetti ripresi;

-sedi di associazioni lgbtqia+, di sexy shops o altri locali che possano rivelare, anche indirettamente, gli orientamenti sessuali dei soggetti inquadrati;

-scuole nel periodo in cui siano adibite a seggi elettorali e che possano quindi rilevare quali soggetti esercitino il diritto di voto e, in via induttiva e presuntiva, le idee politiche in funzione delle relazioni con eventuali candidati o rappresentanti di partiti e movimenti politici.

Non sono disponibili mappe, planimetrie ubicative o altri elaborati grafici.

Fermo restando la scadenza della presente valutazione alla data del 3/2/2027 e della conseguente necessità di aggiornarnamento, si consiglia di verificare periodicamente, con controlli a campione di spezzoni di registrazioni casuali, l'effettiva necessità delle telecamere e dell'area ripresa ai fini dell'attività di polizia e la natura e quantità dei dati registrati a intervalli di tempo oppure in sede di verifica a tempo.

Sulla base dell'area di ripresa e dei sistemi di sicurezza adottati e illustrati in precedenza, allo stato non si ritiene che si possano adottare ulteriori misure per la minimizzazione dei dati e la sicurezza del trattamento dei dati.

B5.3.2 IMPIEGO DELLE TELECAMERE MOBILI OCCULTABILI/FOTOTRAPPOLE (RISCHIO §55)

Nel sistema valutato sono presenti **n. 4 Reolink Go Ranger PT 4K**, con le caratteristiche indicate nella relazione tecnica allegata (-allegato 1-).

Si è rilevato che sono inquadrate aree e contesti che possono rivelare informazioni relative all'attività lavorativa dei dipendenti del titolare degli interessati e ciò costituisce un elemento di rischio da valutare attentamente sia per l'effettiva necessita e sia nel quantitativo di dati acquisiti e nel tempo del trattamento (Linee guida videosorveglianza 9.3.1 e 9.3.2 e art. 25 c. 2 d. lgs. 51/2018), aspetto superabile con l'esclusione ovvero con la modifica del settore inquadrato.

B5.3.3 IMPIEGO DELLE TELECAMERE INSTALLABILI SUI VEICOLI/DASHCAM (RISCHIO §56)

Il titolare del trattamento ha dichiarato che non sono presenti telecamere mobili installabili sui veicoli/dashcam e quindi non si faranno ulteriori valutazioni.

B5.3.4 IMPIEGO DEI SISTEMI DI SANZIONAMENTO MOBILI BASATI SU TELECAMERE (RISCHIO §57)

Il titolare del trattamento ha dichiarato che non sono impiegati sistemi di sanzionamento basati su sistemi di ripresa di immagini fisse e mobili.

B5.3.5 IMPIEGO DELLE TELECAMERE INDOSSABILI/BODYCAM (RISCHIO §58)

Il titolare del trattamento ha dichiarato che non sono presenti telecamere mobili indossabili/body cam e quindi non si faranno ulteriori valutazioni.

B5.3.6 IMPIEGO DEI SISTEMI DI RIPRESA AEREA (RISCHIO §59)

Il titolare del trattamento ha dichiarato che non sono presenti telecamere mobili indossabili/body cam e quindi non si faranno ulteriori valutazioni.

B5.4 Valutazione dei sistemi di localizzazione remota

B5.4.1 SICUREZZA INTRINSECA E POSIZIONAMENTO (RISCHIO §60)

Sono sistemi che attraverso connessioni radio private o traffico dati consentono di localizzare le singole persone attraverso il proprio apparato radio ovvero i veicoli da remoto.

Il titolare del trattamento ha dichiarato che non sono presenti di localizzazione remota che quindi non sono valutati in questa sezione..

B5.5 Criticità della sezione 5 e quantificazione del rischio

Posizionamento delle telecamere di contesto fisse (rischio §51)

Il posizionamento consente di ottenere informazioni relative all'attività lavorativa dei dipendenti del titolare e ciò costituisce un rischio da verificare e limitare al massimo.

CALCOLO DEL RISCHIO §51	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	0,50

Posizionamento delle telecamere di osservazione orientabili (rischio §52)

Il posizionamento consente di ottenere informazioni relative all'attività lavorativa dei dipendenti del titolare e ciò costituisce un rischio da verificare e limitare al massimo.

CALCOLO DEL RISCHIO §52	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	0,50

Posizionamento delle telecamere di rilevamento veicoli e lettura targhe (rischio §53)

Il posizionamento non evidenzia particolari criticità.

CALCOLO DEL RISCHIO §53	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Posizionamento dei sistemi di rilevamento transiti in ZTL/AP (rischio §54)

Il posizionamento non evidenzia particolari criticità.

CALCOLO DEL RISCHIO §54	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

Impiego delle telecamere mobili occultabili/fototrappole (rischio §55)

Il posizionamento consente di ottenere informazioni relative all'attività lavorativa dei dipendenti del titolare e ciò costituisce un rischio da verificare e limitare al massimo.

CALCOLO DEL RISCHIO §55	Indice potenziale di magnitudo	1,00	Indice stimato di pericolo	0,50

Impiego delle telecamere installabili sui veicoli/dashcam (rischio §56)

Non si può definire l'area di posizionamento e quindi quantificare il rischio.

CALCOLO DEL RISCHIO §56	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Impiego dei sistemi di sanzionamento mobili basati su telecamere (rischio §57)

Non si può definire l'area di posizionamento e quindi quantificare il rischio.

CALCOLO DEL RISCHIO §57	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Impiego delle telecamere indossabili/bodycam (rischio §58)

Non si può definire l'area di posizionamento e quindi quantificare il rischio.

CALCOLO DEL RISCHIO §58	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Impiego dei sistemi di ripresa aerea/droni (rischio §59)

Non si può definire l'area di posizionamento e quindi quantificare il rischio.

CALCOLO DEL RISCHIO §59	Indice potenziale di magnitudo	n.d.	Indice stimato di pericolo	//

Valutazione dei sistemi di localizzazione remota (rischio §60)

Non si rilevano particolari criticità nei sistemi di posizionamento.

CALCOLO DEL RISCHIO §60	Indice potenziale di magnitudo	0,00	Indice stimato di pericolo	//

B5.5 Piano di riduzione del rischio della sezione 5

Per ridurre il rischio del nuovo trattamento di cui alla presente valutazione d'impatto-DPIA, si segnala al titolare del trattamento e al RPD/DPO l'opportunità di rimediare in tempi brevi, nel rispetto dei principi di accountability (art. 24 GDPR) e di legalità e correttezza dei trattamenti per finalità di polizia (art. 15 d. lgs. 51/2018), alle criticità evidenziate nel paragrafo precedente.

Fermo restando la piena autonomia del titolare, si suggeriscono alcune attività che potrebbero essere adottate in tempi brevi e da verificare entro la prossima revisione della presente valutazione-DPIA, fissata fra 180 giorni ossia entro il 3/2/2027.

Sezione B5-Valutazione del posizionamento del sistema di ripresa		**Risk mitigation**
RISCHIO	**MISURE DI MITIGAZIONE DEL RISCHIO**	
§51	*variare il posizionamento delle telecamere di contesto in modo che non siano acquisite informazioni relative all'attività lavorativa dei dipendenti del titolare degli interessati;*	
§52	*variare il posizionamento delle telecamere d'osservazione in modo che non siano acquisite informazioni relative all'attività lavorativa dei dipendenti del titolare degli interessati;*	
§53	*nessuna necessaria;*	
§54	*nessuna necessaria;*	
§55	*variare il posizionamento delle telecamere d'osservazione in modo che non siano acquisite informazioni relative all'attività lavorativa dei dipendenti del titolare degli interessati;*	
§56	*nessuna necessaria;*	
§57	*nessuna necessaria;*	
§58	*nessuna necessaria;*	
§59	*nessuna necessaria;*	
§60	*nessuna necessaria.*	
Indice di vulnerabilità stimato (Vu§5): 0,00-non necessarie		

B5.6 Calcolo del rischio finale della sezione 5

Il rischio complessivo, con le procedure e i riferimenti indicati in precedenza, in attesa di ulteriore verifica alla prossima valutazione d'impatto, che consenta di stimare la vulnerabilità del sistema durante il funzionamento, all'esito dell'applicazione delle misure proposte per la riduzione del rischio e delle ulteriori che saranno adottate di propria iniziativa dal titolare, anche sulla base di eventuali indicazioni del responsabile per la protezione dei dati personali (RPD/DPO), risulta come segue:

Sezione B5-Valutazione del posizionamento del sistema di ripresa				**Risk evaluation**
RISCHIO	**ELEMENTO VALUTATO**	**MAGNITUDO**	**PERICOLO**	
§51	Posizionamento delle telecamere di contesto fisse	1,00	0,50	
§52	Posizionamento delle telecamere di osservazione orientabili	1,00	0,50	
§53	Posizionamento delle telecamere di rilevamento veicoli e lettura targhe	0,00	//	
§54	Posizionamento dei sistemi di rilevamento transiti in AP/ZTL	0,00	//	
§55	Impiego delle telecamere mobili occultabili/fototrappole	1,00	0,50	
§56	Impiego delle telecamere installabili sui veicoli/dashcam	n.d.	//	
§57	Impiego dei sistemi di sanzionamento mobili basati su telecamere	n.d.	//	
§58	Impiego delle Telecamere indossabili/bodycam	n.d.	//	
§59	Impiego dei sistemi di ripresa aerea/droni	n.d.	//	
§60	Valutazione dei sistemi di localizzazione remota	0,00	//	
Rischio emergente della sezione (Re§5)		3,00(*)	2,00(*)	**6,00-medio**
Indice di vulnerabilità (Vu§5)	**0,00**	**Rischio residuo (Rr§5)**		**6,00-medio**
Parere del RPD/DPO:		*vedasi eventuale giudizio allegato.*		
Giudizio del titolare del trattamento (DC):		*vedasi giudizio finale.*		

(*) Il rischio è limitato al valore massimo di 5 sia per la magnitudo e sia per il pericolo.

Sezione B6-Conclusioni

Sulla base delle considerazioni svolte in precedenza si riepilogano di seguito i rischi per ogni sezione.

Quantificazione finale del rischio - Risk evaluation				
RISCHI PER AREE DI VALUTAZIONE	**RISCHIO EMERGENTE**	**MISURE DI ATTENUAZIONE**	**RISCHIO RESIDUO**	**VALUTAZIONE PREVENTIVA**
Sezione B1-Descrizione generale del trattamento	12,50-alto	0,25-adeguate	3,13-medio	NO
Sezione B2-Valutazione della proporzionalità del trattamento	21,00-alto	0,25-adeguate	5,25-medio	NO
Sezione B3-Analisi del rischio sui diritti e le libertà delle persone	10,50-rilevante	0,25-adeguate	2,63-medio	NO
Sezione B4-Valutazione degli strumenti del progetto operativo	0,50-basso	0,50-parzialmente adeguate	0,25-basso	NO
Sezione B5-Valutazione del posizionamento dei sistemi di ripresa	6,00-medio	0,00-non necessarie	6,00-medio	NO
ALTRI RISCHI	**PRESENZA**			**VALUTAZIONE PREVENTIVA**
UAS-droni	NO			//
Bodycam	NO			//
Revisione:	**entro il 3/2/2027.**			
Parere del RDP/DPO:	non presente alla data di emissione del presente documento.			
Eventuale commento sulla valutazione:	//			

B6.2 Prescrizioni generali

B6.2.1 FORMAZIONE

L'obbligo di formazione previsto dalla vigente normativa (art.29 e 32 GDPR) che costituisce un dovere generale nell'ambito del principio di accountability, rende necessario non solo un percorso di retraining e aggiornamento per estendere a tutti i soggetti coinvolti nel trattamento con i sistemi di videosorveglianza fissi e mobili inclusi i sistemi di lettura targhe dei veicoli eventualmente utilizzati anche a fini sanzionatori, impiegati sul proprio ambito territoriale, la conoscenza delle procedure e delle cautele da adottare per la tutela dei dati e la corretta gestione del trattamento dei dati.

Si da atto che in data è stata svolta attività formativa come misura di attenuazione del rischio in esecuzione delle indicazioni della precedente valutazione d'impatto sulla protezione dei dati-DPIA.

B6.2.2 VERIFICA DEL RISCHIO

Per le considerazioni sopra indicate si ritiene di doversi rivalutare il trattamento entro 180 giorni dalla data del presente documento e quindi entro il 3/2/2027, salvo variazioni dei mezzi, delle risorse e delle finalità ovvero di qualsiasi altro elemento qui valutato, che renderebbe necessario una

rivalutazione anticipata secondo il giudizio del titolare del trattamento (DC) o del responsabile per la protezione dei dati personali (RPD/DPO).

B6.2.3 ADEGUAMENTI URGENTI

Nei successivi aggiornamenti che si raccomandano di svolgere prima della scadenza, come indicato nel paragrafo precedente, sarà verificata sul campo la necessità di ulteriori adeguamenti in applicazione del ciclo di Deming, nel frattempo si invita il titolare del trattamento (DC) e il responsabile della protezione dei dati (RPD/DPO) a segnalare senza ritardo qualsiasi ulteriore elemento di criticità che dovesse essere rilevato.

Sezione C1-Documenti allegati

C1.1 relazione tecnica e descrittiva del sistema di videosorveglianza (-allegato 1-);

C1.2 pannello informativo "area videosorvegliata" (-allegato 2-) in duplice formato verticale ed orizzontale;

C1.3 informativa sul trattamento dei dati mediante il sistema di videosorveglianza (-allegato 3-);

C.1.4 proposta landing privacy page del Comune di Santeramo in Colle (-allegato 4-);

C.1.5 eventuale parere del responsabile alla protezione dei dati personali (RDP/DPO) (-allegato 5-).

Santeramo in Colle, 7/8/2026

Il revisore della valutazione	Il perito valutatore del rischio

Il soggetto referente designato per i trattamenti esclusi dalla disciplina del GDPR	Per il titolare del trattamento
il della Polizia Locale comm. sup. dott. Vincenzo Caporusso	*il sindaco* avv. Vincenzo Luciano Casone
VINCENZO CAPORUSSO 14/08/2026 10:07:10 UTC+0200	Vincenzo Luciano Casone 14.08.2026 08:58:42 UTC

Signed with NamirialSign