

Accordo Di Contitolarità Del Trattamento Dati Personali Per La Gestione In Forma Associata Del Servizio Di Polizia Locale

tra

Il **Comune di Paladina**, C.F. 80028060160, rappresentato dal Sindaco pro-tempore, dati di contatto: tel. 0356313011 - PEC: comunepaladina@legalmail.it.

Il **Comune di Mozzo**, C.F. 00707040168, rappresentato dal Sindaco pro-tempore, dati di contatto: tel. 0354556611 - PEC: comune.mozzo@pec.regione.lombardia.it

1 Premessa

Considerando che la Legge Regionale 6/2015 promuove lo svolgimento in forma associata della funzione di polizia locale e il coordinamento tra i servizi.

Che le gestioni associate costituiscono un importante strumento per garantire l'applicazione dei principi di sussidiarietà, adeguatezza e differenziazione nella gestione delle funzioni e per dare una risposta migliore sul piano dell'efficienza, dell'efficacia ed economicità della gestione dei servizi e che:

La gestione unificata del servizio di polizia locale comporta il trattamento di dati personali come definiti all'art. 4 del Regolamento UE 2016/679.

L'espletamento dell'attività descritta all'interno della Convenzione tra le Parti comporta anche il trattamento di dati personali effettuato secondo quanto previsto dal Decreto Legislativo 18 maggio 2018, n. 51, in attuazione della direttiva (UE) 2016/680 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;

il servizio utilizza per la gestione dei dati un sistema informativo e un impianto di gestione della videosorveglianza in cui i dati sono trattati dal Servizio Intercomunale di Polizia Locale;

la titolarità del dato non è riconducibile ad un singolo ente, per i motivi sopra esposti;

gli enti che hanno costituito il servizio intercomunale di polizia locale determinano congiuntamente le finalità e le modalità di gestione dei dati degli utenti, come stabilito nella convenzione sottoscritta tra le parti.

Che ai sensi dell'art. 26 del Regolamento UE 2016/679 e dell'art. 17 del d.lgs. 51/2018, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Gli stessi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro a cui i titolari del trattamento sono soggetti.

Nell'ambito delle rispettive responsabilità, i Contitolari dovranno adempiere ai propri obblighi conformemente ai contenuti del presente accordo e ai dettami delle normative in materia di trattamento dei dati personali ed ai dettami delle autorità garanti.

L'accordo in oggetto riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.

2 Oggetto

Il presente Accordo disciplina, ai sensi dell'articolo 26 del Regolamento UE 2016/679, i compiti e le responsabilità in relazione al trattamento dei dati del servizio di Polizia Locale determinati dagli obblighi di legge. Attraverso il presente accordo le parti disciplinano anche i compiti e le regole di gestione dell'impianto di videosorveglianza.

3 Riferimenti Normativi

Il presente accordo risponde ai seguenti requisiti normativi:

- Reg. UE 2016/679 del 27 aprile 2016 (GDPR - General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- D. Lgs 30 giugno 2003 n. 196 recante "Codice in materia di protezione dati personali" e successive modificazioni con particolare riferimento al D. Lgs 10 agosto 2018 n. 101;
- D. Lgs del 10 agosto 2018 n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo;
- D. Lgs 18 maggio 2018 n. 51, attuazione della direttiva (UE) 2016/680, 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;
- Linea guida WP29, Parere 1/2010 sui concetti di "titolare del trattamento" e "responsabile del trattamento" (WP169);
- Linee guida 3/2019 emanate dall'EDPB sul trattamento dei dati personali attraverso dispositivi video.

- Le linee guida 7/2020 del 2 settembre 2020 emanate dall'EDPB (European Data Protection Board) che specificano il ruolo di titolari e contitolari nonché dei responsabili del trattamento.

Acronimi e Definizioni

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) ora EDPB (European Data Protection Board)
RPD/DPO	Responsabile della protezione dei dati (Data Protection Officer)
Responsabile	Responsabile del trattamento ex art. 28 GDPR la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
violazione dei dati personali	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
DPIA: Data Protection impact assessment	Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui possono essere trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l'autorità di controllo nel caso in cui le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

4 Ambito del trattamento

Il presente accordo ha ad oggetto i dati personali, anche appartenenti a categorie particolari, e quelli relativi agli impianti di videosorveglianza installati nei comuni convenzionati, trattati dal Servizio Intercomunale di Polizia Locale regolamentato dalla "Convenzione per l'esercizio associato delle funzioni di polizia locale e protezione civile" sottoscritta dai rappresentanti legali dei Comuni.

Per l'erogazione delle prestazioni oggetto della Convenzione, verranno raccolti e trattati dati personali laddove necessari ed indispensabili rispetto al perseguimento delle obbligazioni derivanti dalle finalità attribuite dalla legge in base ai seguenti presupposti di liceità:

- 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;

- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento in base ai regolamenti e alle leggi dello Stato e del diritto dell'Unione Europea;

Le Parti determinano congiuntamente che la finalità del trattamento è descritta nella convenzione sottoscritta e riguarda:

- la gestione associata è finalizzata al raggiungimento di maggiore efficienza e maggiore specializzazione nello svolgimento delle attività ricomprese nelle funzioni di Polizia Locale e nella funzione consistente nelle attività in ambito comunale di pianificazione di protezione civile e di coordinamento dei primi soccorsi, al miglioramento della qualità dei servizi resi ai cittadini, alla graduale unificazione delle norme regolamentari, alla omogeneità delle modalità operative, nonché alla promozione di una cultura professionale e di una formazione comune tra il personale.
- un migliore utilizzo delle risorse umane e delle risorse strumentali.
- fa parte dei fini della presente convenzione la promozione di un sistema integrato di sicurezza dei cittadini, anche attraverso lo sviluppo di forme di collaborazione e di sinergia con le altre forze di polizia operanti sul territorio.

Ciascuno degli Enti garantisce il rispetto delle disposizioni di legge, in particolare la liceità dei trattamenti di dati da esso effettuati, compresi quelli effettuati in contitolarità. Le parti adottano tutte le misure tecniche e organizzative necessarie affinché i diritti degli interessati, in particolare ai sensi degli articoli da 12 a 22 del GDPR, possano essere garantiti in qualsiasi momento entro i termini di legge.

5 Compiti e responsabilità

Le parti in seguito alla sottoscrizione del presente accordo intendono gestire i dati relativi al servizio di polizia locale stante le medesime/correlate finalità e modalità del trattamento definite, condividendo sia il personale dell'ufficio di polizia sia alcuni asset utilizzati per il trattamento dei dati quali il software di gestione delle sanzioni del codice della strada e l'impianto di videosorveglianza e di rilevazione delle targhe installato sul territorio degli Enti Aderenti.

Questo comporta la necessità di definire alcuni compiti e responsabilità come di seguito riportati:

- a) Ogni singolo contitolare è responsabile della corretta applicazione delle prescrizioni e delle indicazioni contenute nel presente documento per le parti di propria competenza..
- b) I Contitolari sono tenuti ad attuare gli adempimenti previsti dal Reg. UE 2016/679 e dalla normativa italiana sul trattamento dei dati (D Lgs 196/2003 come modificato dal Dlgs 101-2018).
- c) Ai singoli contitolari compete l'attuazione di regole e procedure di sicurezza nella gestione dei dati ed attuare le disposizioni emanate da AGID a cui gli enti pubblici sono tenuti ad adeguarsi nei trattamenti effettuati dal Comune nell'ambito del proprio territorio.

- d) I Contitolari si impegnano a trattare i dati personali degli interessati gestiti nelle banche dati del servizio Intercomunale di Polizia Locale per le finalità per le quali gli stessi sono stati raccolti.
- e) Eventuali reclami o richieste di esercizio dei diritti degli interessati verranno gestiti in ottemperanza alle prescrizioni del GDPR da parte dei singoli enti, con il supporto del Servizio Unificato di Polizia Locale.
- f) Le parti concordano che è compito dell'Ufficio Intercomunale di Polizia Locale formare gli operatori autorizzati in materia di corretta gestione dei dati in ottemperanza alla normativa sulla protezione dei dati.
- g) Le parti concordano che è compito di ciascun Ente Contitolare attuare le corrette regole di gestione dei dati contenute nel presente accordo o contenute nelle normative di legge applicabili.

La tipologia di trattamento dei dati di cui sopra verrà gestita secondo lo schema seguente:

Trattamenti	Gestione del servizio di <i>Polizia municipale e polizia amministrativa locale</i>	Gestione dei dati del personale di polizia	Gestione della videosorveglianza
Finalità del trattamento	Svolgimento delle attività di polizia municipale e amministrativa locale (inserimento nelle anagrafiche e nei database informatici comunali; svolgere attività di polizia amministrativa locale, annonaria e commerciale; elaborazione di statistiche interne gestione dell'ordine pubblico e della sicurezza; controllo del territorio; gestione e applicazione di sanzioni amministrative e di eventuali ricorsi; gestione di incassi e pagamenti; gestione e rilascio di permessi per soggetti diversamente abili; controllo per il rispetto delle regole d'igiene, di attività edili, in materia di ambiente, sanità e di polizia mortuaria).	Gestione congiunta dei dati del personale di polizia per lo svolgimento delle attività di polizia municipale e amministrativa locale.	Gestione delle immagini rilevate dall'impianto di videosorveglianza attivo per finalità di sicurezza e tutela del territorio e del patrimonio comunale, oltre che di prevenzione e repressione di illeciti.
Tipologia di dati	Dati personali comuni; Dati particolari (dati idonei a rivelare lo stato di salute); Dati relativi a condanne penali e reati ai sensi dell'art. 10 GDPR.	Dati personali comuni (identificativi e di contatto); Categorie particolari di dati personali (dati idonei a rivelare lo stato di salute); Dati relativi a condanne penali e reati ai sensi dell'art. 10 GDPR.	Dati personali comuni; Dati particolari.

Rapporto giuridico tra le Parti	Contitolarità.	Contitolarità.	Contitolarità.
Informativa da realizzare	Informativa Privacy – Gestione del servizio di Polizia municipale e polizia amministrativa locale (parte integrante e sostanziale del presente accordo di contitolarità – allegato 1).	Informativa Privacy – Personale (parte integrante e sostanziale del presente accordo di contitolarità – allegato 2).	Informativa Privacy – Gestione del servizio di Polizia municipale e polizia amministrativa locale (parte integrante e sostanziale del presente accordo di contitolarità – allegato 1).
Soggetto addetto alla consegna dell'informativa	Il Contitolare che per primo ha il contatto con l'interessato. Inoltre, l'informativa sarà resa disponibile sul sito istituzionale di ogni Contitolare.	Il Contitolare che per primo ha il contatto con l'interessato.	Il Contitolare che per primo ha il contatto con l'interessato. Inoltre, l'informativa sarà resa disponibile sul sito istituzionale di ogni Contitolare. Inoltre, nei luoghi sottoposti a videosorveglianza, sarà presente un modello semplificato di informativa “minima”.
Soggetto principale per la gestione delle richieste dell'interessato	Il Contitolare a cui si rivolge l'interessato.	Ogni singolo Ente titolare del rapporto contrattuale con l'operatore di polizia.	Il Contitolare a cui si rivolge l'interessato.
Data Breach	Gestione congiunta per la notifica all'Autorità Garante da parte del Contitolare presso cui avviene la violazione. Notifica all'Autorità Garante da parte del Contitolare presso cui avviene la violazione. Se necessaria comunicazione agli interessati, a carico del Contitolare presso cui avviene la violazione.	Gestione congiunta per la notifica all'Autorità Garante da parte del Contitolare presso cui avviene la violazione. Notifica all'Autorità Garante da parte del Contitolare presso cui avviene la violazione. Se necessaria comunicazione agli interessati, a carico del Contitolare presso cui avviene la violazione.	Gestione congiunta per la notifica all'Autorità Garante da parte del Contitolare presso cui avviene la violazione. Notifica all'Autorità Garante da parte del Contitolare presso cui avviene la violazione. Se necessaria comunicazione agli interessati, a carico del Contitolare presso cui avviene la violazione.
DPO di riferimento	DPO del Contitolare a cui si rivolge l'interessato, fornendo comunque comunicazione ai DPO degli altri Contitolari.	DPO del Contitolare a cui si rivolge l'interessato, fornendo comunque comunicazione al DPO dell'altro Contitolare.	DPO del Contitolare a cui si rivolge l'interessato, fornendo comunque comunicazione ai DPO degli altri Contitolari.

6 Gestione dei Dati

La “contitolarità” è riferita all'acquisizione congiunta e/o disgiunta e/o al conseguente trattamento dei dati acquisiti e trattati dal Servizio Intercomunale di Polizia Locale per le

finalità sopra riportate, intendendosi per "trattamento" qualunque operazione o complesso di operazioni effettuate con o senza l'ausilio di strumenti elettronici.

Ogni singolo ente ha la responsabilità di attuare le misure di sicurezza necessarie per garantire una adeguata protezione delle banche dati trattate presso la propria sede o territorio attinenti al servizio di Polizia locale in base ad una valutazione dei rischi e ad una eventuale DPIA (Data Protection Impact Assessment).

Ciascuna parte, per i dati nella propria diretta disponibilità, è responsabile dell'adozione di misure di sicurezza coerenti con quanto indicato all'art. 32 del GDPR.

Le misure di sicurezza investono anche i fascicoli e gli atti conservati su supporto cartaceo. Le regole adottate sono comunicate dal comandante dell'Ufficio Unificato di Polizia Locale ai Contitolari del trattamento attraverso una procedura scritta.

7 Comunicazioni relative alle politiche di protezione dei dati

Il Comune di Paladina predispone i modelli di informativa relativi al trattamento dei dati del servizio unificato di polizia locale e li trasmette ai DPO dei Contitolari per eventuali osservazioni.

Ogni singolo ente è responsabile di attuare le procedure di comunicazione agli interessati delle politiche di trattamento dei dati, attraverso le informative previste dagli artt. 13 e 14 del Reg. UE 2016/679.

Il contenuto dell'informativa relativa al trattamento delle informazioni identifica le politiche adottate dal servizio ed è condivisa ed adottata dai Contitolari del trattamento.

La gestione della stessa prevede le seguenti regole:

- L'informativa dei Contitolari relativa agli utenti del servizio di polizia locale verrà esposta presso gli sportelli del servizio e pubblicata sul sito istituzionale dei singoli Enti;
- Nei modelli di presentazione di una istanza o raccolta dei dati relativi al servizio di Polizia Locale (ex modello accesso agli atti, richiesta contrassegno invalidi ecc), ove sia prevista la comunicazione dell'informativa, dovrà essere inserita una "informativa minima" univoca dei Contitolari relativa al trattamento dei dati;
- L'informativa dettagliata relativa all'impianto di videosorveglianza del servizio unificato di Polizia Locale deve essere pubblicata sul sito istituzionale dei singoli Enti;
- L'informativa in prossimità delle aree video sorvegliate (cartelli segnaletici) identifica i contitolari del trattamento ed è posizionata prima che il cittadino acceda allo spazio monitorato. Quest'ultima deve essere conforme alle linee guida 3/2019 emanate dall'EDPB sul trattamento dei dati personali attraverso dispositivi video.

8 Diritti degli interessati

Gli interessati possono far valere i loro diritti ai sensi degli articoli da 15 a 22 del GDPR nei confronti degli enti che hanno costituito il servizio congiunto di Polizia Locale intercomunale. I diritti dell'interessato sono sempre esercitabili, salvo che i Contitolari non siano in grado di identificare l'interessato (esempio dati anonimi).

Il Contitolare al quale è stata presentata l'istanza deve dare seguito alle eventuali richieste di esercizio dei diritti degli interessati entro un mese dal ricevimento di tale richiesta. Il termine può essere prorogato a due mesi, tenuto conto della complessità e del numero di richieste, informando l'interessato dei motivi del ritardo.

Se le richieste pervengono a mezzo elettronico, le risposte verranno fornite, ove possibile, con mezzi elettronici. Il Regolamento prevede altresì la possibilità di risposta orale, ove così richieda l'interessato.

Nel caso in cui il Contitolare non possa dare seguito alla richiesta nei termini previsti deve comunque informare l'interessato e fornire le motivazioni dell'inottemperanza, informandolo della possibilità di proporre reclamo al Garante o ricorso all'Autorità Giudiziaria.

In via generale le richieste per l'esercizio dei diritti degli interessati sono gratuite; tuttavia, se le richieste sono manifestamente infondate o eccessive, il Titolare può prevedere un addebito o un contributo spese tenuto conto dei costi amministrativi sostenuti per fornire le informazioni oppure rifiutare di soddisfare la richiesta. L'onere di dimostrare l'infondatezza o il carattere eccessivo della richiesta è in capo al Contitolare del trattamento.

Gestione delle istanze per far valere i diritti sul trattamento dei dati: Le istanze relative al trattamento dei dati verranno accolte e gestite dal Comando di Polizia Unificato nella persona del comandante, il quale, ove necessario, si avvarrà del supporto normativo e procedurale del DPO (Responsabile della Protezione dei Dati) del comune in cui l'utente ha presentato l'istanza.

Le risposte alle istanze inerenti al trattamento dei dati del servizio Intercomunale di Polizia Locale con riferimento a:

- attuazione dei diritti degli interessati
- misure di sicurezza attuate per la protezione dei dati del servizio
- applicazione dei principi previsti dalla normativa

verranno gestite dal Comando del Servizio Unificato, avvalendosi del supporto della struttura amministrativa degli enti in cui le banche dati sono trattate e del DPO dell'ente in cui è stata presentata istanza.

Nel caso in cui l'istanza sia presentata direttamente al Responsabile della Protezione dei dati di uno dei Contitolari, è compito di quest'ultimo gestirla, attenendosi alle disposizioni del Reg. UE 2016/679 e coinvolgendo il Comando di Polizia Locale.

9 Registro dei trattamenti

La documentazione ai sensi dell'art. 5 del GDPR, che serve come prova del corretto trattamento dei dati, deve essere conservata da ciascuna delle parti oltre la cessazione del presente accordo, conformemente ai poteri e agli obblighi di legge.

In particolare, ogni comune dovrà aggiornare il registro dei trattamenti indicando i soggetti contitolari del trattamento.

10 Gestione dei fornitori del servizio di Polizia Locale

Le Parti si informano reciprocamente e con tempestività in merito a qualsiasi modifica relativa ai servizi dell'Ufficio di Polizia Locale che comporti il coinvolgimento, la sostituzione

o l'aggiunta di fornitori che, direttamente o indirettamente, trattano dati personali per conto dei Comuni aderenti o del Servizio Intercomunale di Polizia Locale.

Le Parti individuano esclusivamente fornitori che garantiscano il pieno rispetto della normativa in materia di protezione dei dati personali, delle misure di sicurezza richieste dall'art. 32 del Regolamento (UE) 2016/679 e delle disposizioni contenute nel presente accordo di contitolarietà.

In ogni caso, le Parti sono tenute a:

- stipulare idonei accordi contrattuali con i fornitori, conformi alla normativa vigente e ai requisiti previsti dall'art. 28 del Regolamento (UE) 2016/679;
- adottare misure di controllo e vigilanza sull'operato dei fornitori, al fine di garantire la protezione e la sicurezza dei dati personali trattati nell'ambito dei servizi dell'Ufficio di Polizia Locale;
- assicurare che tali obblighi siano rispettati anche in caso di servizi aggiuntivi affidati a terzi.

Nel caso in cui il Servizio di Polizia Locale intercomunale decida di esternalizzare servizi che prevedono il trattamento di dati personali, si distinguono le seguenti situazioni:

1. **Servizio esternalizzato da uno dei Comuni aderenti alla convenzione** In questo caso, la gestione del fornitore, sotto il profilo della regolamentazione prevista dal GDPR, resta in capo al Comune titolare del contratto, che assume gli obblighi di nomina del Responsabile del trattamento e di vigilanza sul suo operato. Le altre Parti devono essere informate e possono richiedere evidenze documentali delle misure adottate.
2. **Servizio esternalizzato direttamente dal Servizio Intercomunale di Polizia Locale** In questo caso, la gestione del fornitore, sotto il profilo della regolamentazione prevista dal GDPR, è in capo all'Ente capofila del Servizio Intercomunale, che provvede alla nomina del Responsabile del trattamento, alla definizione delle istruzioni operative e alla verifica delle misure di sicurezza adottate. Gli altri Comuni aderenti collaborano fornendo informazioni utili e segnalando eventuali criticità.

11 Valutazione di impatto art. 35 GDPR (DPIA)

Ciascun Comune contitolare, per quanto di propria competenza, è tenuto a valutare se le operazioni di trattamento effettuate nell'ambito dei servizi di Polizia Locale (comunale o intercomunale) richiedano lo svolgimento di una **Valutazione di Impatto sulla Protezione dei Dati (DPIA)** ai sensi dell'art. 35 del Regolamento (UE) 2016/679.

A tal fine, ogni Comune contitolare si impegna a:

- a) **Identificare le operazioni di trattamento che presentano rischi elevati**, avvalendosi, ove necessario, dei fornitori che gestiscono la rete informatica, gli applicativi gestionali, i sistemi di videosorveglianza e gli impianti di registrazione delle immagini.
- b) **Valutare la presenza di rischi elevati** secondo i criteri previsti dalle Linee Guida del WP29 e dalle indicazioni del Garante per la protezione dei dati personali, tenendo conto delle specificità organizzative e operative del proprio ente. Qualora emergano trattamenti che richiedono una DPIA, il Comune contitolare competente avvia la valutazione, acquisendo le informazioni tecniche necessarie dai fornitori coinvolti. L'esito della DPIA viene condiviso

con gli altri contitolari, affinché possano tenerne conto nelle rispettive attività di trattamento correlate.

c) **Adottare e comunicare agli altri contitolari** eventuali misure di sicurezza aggiuntive ritenute necessarie per la corretta gestione dei dati personali e delle informazioni trattate nell'ambito del servizio di Polizia Locale, incluse quelle derivanti dall'esito della DPIA.

11.1 Ruolo del Comune capofila

Il Comune capofila, nell'ambito delle attività di coordinamento del Servizio Intercomunale di Polizia Locale, garantisce:

- la **circolazione delle informazioni** tra i contitolari in merito alle DPIA effettuate dai singoli Comuni;
- il **supporto organizzativo** per la raccolta di elementi tecnici utili alle valutazioni di impatto;
- la **coerenza complessiva** delle misure adottate dai contitolari, al fine di assicurare un livello omogeneo di protezione dei dati personali nell'intero servizio intercomunale.

12 Privacy by Design e by default

I singoli Comuni contitolari, ciascuno per quanto di propria competenza, **individuano, adottano e documentano** le misure tecniche e organizzative adeguate a garantire che il trattamento dei dati personali effettuato nell'ambito del Servizio Intercomunale di Polizia Locale sia conforme al Regolamento (UE) 2016/679 e idoneo a ridurre i rischi per gli interessati. Ogni Comune deve essere in grado di **dimostrare l'adeguatezza** delle misure implementate, in coerenza con i principi di accountability, privacy by design e privacy by default.

Il Comune capofila del Servizio Intercomunale, nell'ambito delle funzioni di coordinamento attribuite dalla convenzione, **fornisce agli altri Comuni contitolari indicazioni, linee guida e soluzioni di riferimento** ritenute idonee per assicurare un livello omogeneo di protezione dei dati personali nell'intero servizio. Tali indicazioni non sostituiscono le responsabilità dei singoli Comuni, che restano autonomamente tenuti a valutare, implementare e dimostrare le misure adottate.

12.1 Progettazione dei nuovi trattamenti

Ogni nuovo trattamento, così come l'introduzione di nuove modalità operative, tecnologie, applicativi o impianti che comportano il trattamento di dati personali, deve essere **progettato e gestito da ciascun Comune contitolare** in modo da garantire un'adeguata protezione dei dati, assicurando che:

- siano raccolti solo i dati necessari rispetto alle finalità perseguite;
- le finalità del trattamento siano chiaramente definite e documentate;
- i periodi di conservazione siano determinati e proporzionati;
- l'accessibilità ai dati sia limitata ai soli soggetti autorizzati.

Il Comune capofila, nell'ambito del coordinamento, **indica agli altri Comuni contitolari** criteri e misure di riferimento utili per garantire che i trattamenti siano conformi ai principi di protezione dei dati per impostazione predefinita. È facoltà di ogni Comune identificare i

criteri con cui adottare le misure di protezione dei dati previste dalle norme di legge o da provvedimenti dell'autorità garante.

13 Data Breach

L'art. 33 del GDPR indica che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 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".

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'art. 4 p.12 del Reg. UE 2016/679 definisce la violazione dei dati personali come una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre elementi ben noti della sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

13.1 Compiti dei Contitolari nel caso di Data Breach

Le parti si impegnano a comunicarsi reciprocamente tramite PEC posta all'attenzione del rappresentante legale e del segretario comunale qualsiasi violazione dei dati personali oggetto del presente accordo (data breach) entro e non oltre 1 giorno lavorativo dal momento di avvenuta conoscenza dell'evento e di confrontarsi e aggiornarsi reciprocamente su quanto accaduto e sugli interventi da attuare.

Nel caso ne ricorrano le condizioni, la notifica al Garante per la protezione dei dati personali compete all'Ente che ha subito il data breach. Il Comando Intercomunale di Polizia Locale collabora mettendo a disposizione le necessarie informazioni e documentazione eventualmente in suo possesso al fine di gestire in modo corretto la segnalazione nei termini di legge (entro 72 ore dal momento in cui ne è venuta a conoscenza).

La gestione dell'incidente viene attivata dall'ente sulla cui infrastruttura o nella cui sede sono installate le banche dati oggetto di violazione seguendo la procedura di data breach adottata dal relativo ente.

In caso di elevato rischio per i diritti e le libertà degli interessati, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio. Ogni Contitolare provvederà a gestire questa attività per le parti di propria competenza.

La comunicazione agli interessati, secondo quanto previsto dall'art. 34 del GDPR, non è richiesta quando:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati.

Se il rischio è grave verrà data comunicazione attraverso pubblicazione dei dati relativi al data breach sui siti istituzionali dei contitolari e se possibile usando gli indirizzi di posta elettronica di cui i contitolari dispongono ognuno per la propria competenza.

Le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679 devono essere condivise tra i contitolari.

14 Responsabilità dei Contitolari

Le Parti sono responsabili per il rispetto delle misure di propria pertinenza al fine di garantire il risarcimento effettivo dell'interessato ai sensi di quanto previsto dalla Normativa Applicabile e dagli articoli 26 e 82 del Regolamento.

Per quanto riguarda il trattamento dei dati personali previsti nell'Accordo, i Contitolari saranno ritenuti solidalmente responsabili nei confronti degli interessati, i quali potranno agire nei confronti di ciascun Contitolare per la tutela dei propri diritti. Ferma restando la responsabilità solidale verso gli interessati, è sin d'ora convenuto che ciascun Contitolare potrà esercitare un'azione di regresso nei confronti degli altri Contitolari per le eventuali sanzioni, multe, ammende o danni derivanti dalla violazione o dall'erronea esecuzione del presente Accordo.

Ciascun Contitolare risponde, invece, in via autonoma ed esclusiva per il danno cagionato dal suo trattamento che violi la normativa europea e nazionale indicata, nonché se ha agito in modo difforme o contrario alle indicazioni contenute nel presente Accordo.

15 Adesione di nuovi Soggetti

Ogni soggetto che intende aderire al Servizio Unificato di Polizia Locale deve sottoscrivere la Convenzione ed accettare il presente Accordo di Contitolarità.

I contitolari informano il Comune Capofila di aver attuato le prescrizioni in materia di trattamento dei dati contenute nel GDPR e nella normativa applicabile.

I dati del nuovo soggetto verranno comunicati ai Contitolari e l'accordo di contitolarità verrà aggiornato e pubblicato sui siti internet degli enti aderenti.

16 Valutazione di impatto per nuovi trattamenti

Per ogni nuova iniziativa che comporti l'utilizzo di nuove tecnologie per il trattamento dei dati, o in caso di modifiche di strumenti del trattamento già adottati (artt. 35 ss. Regolamento UE 2016/679 e artt. 23 e 24 D.Lgs. 51/2018), i Contitolari si impegnano a collaborare per la valutazione dei rischi connessi e delle misure tecniche ed organizzative da adottare a tutela dei dati personali.

17 Segretezza e Confidenzialità

I Contitolari si impegnano a considerare strettamente confidenziale tutto il materiale generalmente non di dominio pubblico di cui possono venire a conoscenza in ragione del rapporto di contitolarità e si impegnano a comunicare e utilizzare tali informazioni solamente per gli scopi previsti dal presente Accordo.

18 Revisione e Comunicazioni del contenuto dell'Accordo

Le parti si impegnano a revisionare il presente accordo in caso di necessità; a tal fine verrà monitorato e revisionato periodicamente per assicurarne l'attualità e l'allineamento alle novità legislative. Il presente Accordo viene meno con la cessazione delle condivise finalità del trattamento da parte dei contitolari o qualora non vi siano più i presupposti di contitolarità. Ai sensi dell'articolo 26 comma 2 del Regolamento UE 2016/679, **il contenuto essenziale del presente accordo è pubblicato sul sito dei Contitolari e in tal modo messo a disposizione degli interessati.**

Per ogni altro aspetto non trattato esplicitamente nel presente accordo, le parti rinviano espressamente al testo del Reg. UE 2016/679 e alla normativa vigente in materia di gestione dei dati personali.

19 Durata

I termini del presente Accordo sono pari a quelli della Convenzione sottoscritta dagli enti per costituire il Servizio Intercomunale di Polizia Locale.