

SCHEMA DI:

**ACCORDO CON GLI ENTI LOCALI PER L'ACCESSO AL SISTEMA INTEGRATO DI SICUREZZA PARTECIPATA (SISP) - (L.R. 6/2015)**

\*\*\*

**la Giunta Regionale della Lombardia**, con sede in Milano - 20124, Piazza Città di Lombardia 1, C.F. 80050050154 e Partita IVA 12874720159, nella persona del Direttore Generale pro-tempore della Direzione Sicurezza

**E**

**l'Ente fruitore (Comune/Unione di Comuni/Città Metropolitana) .....**, qui rappresentato dal Sindaco/Presidente pro-tempore, in qualità di Legale Rappresentante

**Premesso che:**

- la legge regionale 1 aprile 2015, n. 6 “Disciplina regionale dei servizi di polizia locale e promozione di politiche integrate di sicurezza urbana”:
  - all’art. 1, comma 1, pone la sicurezza urbana tra le condizioni primarie per un ordinato svolgimento della vita civile e nel pieno rispetto dell'esclusiva competenza statale in materia di ordine pubblico e sicurezza;
  - all’art. 3, comma 1, lettera a), prevede che la Regione promuova la collaborazione istituzionale con gli enti locali, territoriali e statali, mediante la stipulazione di accordi, in modo da assicurare, nel rispetto delle competenze di ciascun soggetto, efficaci interventi di sicurezza urbana, polizia amministrativa, tutela ambientale, sicurezza stradale e protezione civile sull'intero territorio regionale;
  - all’art. 5, comma 1, lettere a) e b), stabilisce che la Regione:
    - a) promuova e sostenga, anche con strumenti finanziari, la realizzazione dei progetti per la sicurezza urbana e incentiva la realizzazione dei patti locali di sicurezza;
    - b) fornisca sostegno all'attività operativa, di formazione e di aggiornamento professionale della polizia locale, promuovendo anche forme di collaborazione con le forze di pubblica sicurezza;

- all'articolo 15, istituisce, al comma 1, nell'ambito dell'organizzazione della Giunta regionale, apposita struttura per la promozione del coordinamento tra i servizi di polizia locale, individuandone, al comma 2, le rispettive competenze, tra cui, come specificato alla lettera b), quella concernente la raccolta e il monitoraggio dei dati inerenti le funzioni di polizia locale, nonché la diffusione dei dati stessi;
- all'articolo 25, comma 2, lettere a) e b), prevede che la Regione promuova la realizzazione, da parte degli enti locali, di progetti finalizzati a sviluppare politiche di sicurezza urbana, per prevenire e contenere fenomeni di disagio sociale, degrado urbano e inciviltà, in rapporto alle peculiari caratteristiche e problematicità di ciascun contesto territoriale;
- Regione Lombardia ha realizzato, mediante la propria società ARIA SpA, a ciò appositamente incaricata, uno strumento informatico denominato Sistema Integrato Sicurezza Partecipata (SISP), rivolto ai Comandi di Polizia locale più strutturati del territorio lombardo, in quanto dotati di un numero di operatori adeguato ad un impiego ricorrente e sistematico di una tale tipologia di sistema;
- trattasi di uno strumento utile al monitoraggio delle criticità urbane, realizzato attraverso la raccolta delle comunicazioni presenti nelle piattaforme *social*;
- il sistema si avvale anche di una collezione di immagini satellitari ad alta risoluzione di nuova e vecchia acquisizione che coprono il territorio di Milano e dei comuni della cintura milanese; su queste immagini possono essere effettuate delle analisi per monitorare il cambiamento nel tempo sul territorio, in termini di abusivismo (edilizio e ambientale);
- i dati raccolti consentono di alimentare un cruscotto multidimensionale di monitoraggio attraverso il quale è possibile condurre l'analisi e la consultazione delle segnalazioni di degrado e insicurezza urbana;
- tale strumento, fortemente innovativo dal punto di vista metodologico e di progettazione, è facilmente consultabile via web tramite browser da una postazione del Comando di polizia locale collegata in rete per l'analisi, con esclusivo riferimento al territorio di propria competenza, delle eventuali segnalazioni di degrado e insicurezze urbane derivanti dai dati *social* e satellitari, rilevanti per la prevenzione e per le attività di Polizia Giudiziaria, ai fini dell'individuazione e repressione dei reati;
- scopo di tale iniziativa è quello di dotare sperimentalmente le Polizie locali più strutturate di uno strumento che contribuisca:
  - a meglio conoscere e indagare il territorio, per individuare fatti e comportamenti in violazione delle norme in materia di sicurezza urbana, anche attraverso le segnalazioni degli utenti;
  - a elaborare la mappa dei siti sensibili del territorio, al fine della predisposizione dei servizi di vigilanza e controllo;

- ad avviare attività di accertamento di violazioni;
- in data 28 maggio 2020, la Direzione Generale “Sicurezza” di Regione Lombardia ha organizzato, con le modalità prescritte nel periodo di emergenza COVID-19, la presentazione del Sistema Integrato Sicurezza Partecipata (SISP), sperimentale per l’anno 2020, acquisendo l’interesse di numerosi Enti locali ad avvalersi di tale strumento, successivamente dotato dei cosiddetti “coni di osservazione” per limitare la visione dei dati al solo territorio di competenza di ciascuna polizia locale;

**Considerata** l’opportunità di sottoscrivere uno specifico accordo con gli Enti interessati, disciplinante le modalità di impiego sperimentale del Sistema Integrato di Sicurezza Partecipata (SISP) per le finalità suddette, con le modalità prescritte, anche con riferimento alla tutela della *privacy*;

**Considerato** che:

- il Garante per la protezione dei dati personali, nelle more della definizione da parte di AGID degli standard di comunicazione e delle regole tecniche, con il provvedimento “Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche” del 2 luglio 2015, conferma le specifiche misure tecniche e organizzative già individuate nelle Linee guida dell'AGID ver.2.0, prescrivendo pertanto alle Pubbliche Amministrazioni l'adozione delle stesse;
- il provvedimento del 2 luglio 2015 di cui al precedente capoverso richiama specificamente le Pubbliche Amministrazioni alla previsione che in caso di violazione dei dati o incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati, le stesse debbano comunicare al Garante tali eventi entro quarantotto ore dalla conoscenza del fatto, mediante redazione dell'apposito modulo da indirizzare a [databrech.pa@pec.gpdp.it](mailto:databrech.pa@pec.gpdp.it);
- Regione Lombardia, attraverso la propria società incaricata ARIA SpA, effettua la supervisione tecnica e il monitoraggio sulle operazioni di accesso e sul sistema in generale, garantendo il costante aggiornamento e la sicurezza dei dati tramite i competenti uffici;
- il presente accordo è conforme alle misure individuate dal Garante per la protezione dei dati personali con il citato provvedimento del 2 luglio 2015;
- in attuazione dell’art. 35, comma 3, lettera b) del d.lgs. 14 marzo 2013, n. 33, recante disposizioni in materia di pubblicità, trasparenza e diffusione di informazioni, Regione Lombardia, con atto n. 5637 del 3 ottobre 2016, ha definito lo schema del presente “Accordo”, aderendo al quale l’ente fruitore può

aver accesso alle informazioni, di propria competenza, contenute nella banca dati d'interesse per lo svolgimento dei suoi compiti istituzionali;

- Il decreto legislativo 18 maggio 2018, n. 51, di attuazione della direttiva (UE) 2016/680 specifica gli ambiti di attività sui trattamenti effettuati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali;

**Convenuto** che, nell'ambito del testo e degli allegati al presente accordo si intendono per:

1. “Codice”: il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003 n. 196 e s.m.i., 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;
2. “CAD”: il Codice dell'Amministrazione Digitale di cui al decreto legislativo 7 marzo 2005 n. 82 e successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217
3. “Responsabile dell’accordo”: soggetto preposto da ciascuna delle Parti alla gestione dei rapporti e delle comunicazioni inerenti all’accordo;
4. “Referente tecnico”: soggetto nominato dalle Parti in sede di stipula dell’accordo e preposto all'attivazione e alla successiva gestione operativa dello scambio dati nonché alla corretta applicazione delle regole di sicurezza tecnico-organizzative previste dall’accordo;
5. “Supervisore”: soggetto nominato dall'ente fruitore preposto al monitoraggio e controllo dell'utilizzo dei servizi d'accesso da parte degli utenti dell'ente di appartenenza;
6. “Amministratore utenze”: soggetto nominato dall'ente fruitore e preposto alla richiesta e revoca delle autorizzazioni di accesso per gli utenti dell'ente di appartenenza;

**Tutto ciò premesso e considerato, convengono e stipulano quanto segue:**

## **ART. 1 - Premesse**

1. Le premesse costituiscono parte integrante e sostanziale del presente accordo.

2. Il presente accordo disciplina i rapporti tra le Parti, al fine di regolare le modalità di accesso al Sistema Integrato di Sicurezza Partecipata (SISP), conformemente ai principi stabiliti dal Codice e dagli *standard* di sicurezza informatica.

## **ART. 2 – Oggetto e finalità**

1. Il presente accordo disciplina, conformemente ai principi stabiliti dal Codice e dagli *standard* di sicurezza informatica, i rapporti tra le Parti, al fine di regolare le modalità di accesso dell'Ente sottoscrittore, in via sperimentale, al Sistema Integrato di Sicurezza Partecipata (SISP), attraverso un cruscotto multidimensionale di monitoraggio del territorio interrogato, mediante accesso riservato, da uno o più operatori di polizia locale, da postazione informatica collegata in rete. Il dispositivo permetterà al Comando di polizia locale:
  - di monitorare le segnalazioni di degrado e insicurezza urbane derivanti dalle piattaforme social;
  - di consultare le immagini satellitari ad alta risoluzione di nuova e vecchia acquisizione che coprono il territorio di Milano e dei comuni della cintura milanese, utili a contrastare l'abusivismo edilizio ed il degrado ambientale;
  - di meglio conoscere e indagare il territorio, per individuare fatti e comportamenti in violazione delle norme in materia di sicurezza urbana, anche attraverso le segnalazioni degli utenti;
  - di elaborare la mappa dei siti sensibili del territorio, al fine della predisposizione dei servizi di vigilanza e controllo;
  - di avviare attività di accertamento di violazioni;
2. L'ente fruitore è autorizzato alla gestione dei propri dati nel rispetto e nei limiti delle finalità istituzionali perseguite e della base normativa che lo legittima per l'acquisizione delle informazioni, come risulta dall'allegato 1. La sussistenza del rispetto di tali presupposti sarà oggetto di verifica preventiva condotta da Regione Lombardia, in qualità di ente erogatore, ogni qual volta il fruitore inoltrerà richiesta di abilitazione all'accesso al sistema SISP.
1. I servizi di accesso ai sistemi informatici, che verranno attivati a seguito della stipula dell'accordo, sono regolati dalle modalità di gestione previste ai successivi articoli e più specificatamente nell'allegato 4.

## **ART. 3 - Impegni dell'Ente sottoscrittore**

1. L'Ente locale ..... (Comune/Unione di Comuni) richiede l'accesso per la fruizione del Sistema integrato di Sicurezza Partecipata (SISP) attraverso il Portale dei Servizi della Direzione (<https://sicurezza.servizirl.it/>).

2. Il/La ..... (Comune/Unione di Comuni) si impegna ad utilizzare il Sistema integrato di Sicurezza Partecipata (SISP), messo gratuitamente a disposizione da Regione Lombardia, secondo quanto specificato nell'Allegato A al presente accordo.
3. Il/La ..... (Comune/Unione di Comuni) si impegna a fornire a Regione il numero e la tipologia, in forma anonima e aggregata, ai soli fini statistici e di valutazione per lo sviluppo delle politiche regionali di sicurezza urbana degli accessi e dei risvolti/utilità operativi solamente per tipologie che l'uso dello strumento ha permesso.

#### **ART. 4 – Soggetti dell'accordo per l'accesso e l'utilizzo del Sistema Integrato di Sicurezza Partecipata (SISP)**

1. Ai fini della corretta applicazione dell'accordo, ciascuna delle Parti nomina un proprio Responsabile dell'accordo, quale rappresentante preposto alla gestione dei rapporti e delle comunicazioni tra le Parti per la gestione del rapporto convenzionale.
2. I nominativi ed i recapiti dei Responsabili dell'accordo sono riportati nell'allegato 2.
3. Rientra nei compiti del Responsabile dell'accordo il mantenimento e la gestione dello stesso in relazione a qualsiasi modifica dovesse generarsi, con scambio di formali comunicazioni, a seguito di evoluzione tecnica e funzionale dei servizi erogati. Inoltre, il Responsabile dell'accordo di Regione Lombardia curerà:
  - a) l'integrazione di ulteriori autorizzazioni di accesso ai dati, secondo le modalità regolate dall'accordo, previa verifica di legittimità sulla base delle disposizioni vigenti;
  - b) il consolidamento della versione aggiornata dell'accordo a seguito di nuovi servizi, adeguamenti tecnici e/o modifiche alla struttura dell'accordo stesso con riferimento anche ad eventuali evoluzioni previste dal CAD;
  - c) la comunicazione all'ente fruitore nel caso in cui siano riscontrati eventuali abusi, anomalie e/o utilizzi non conformi ai fini istituzionali per il perseguimento dei quali è ammesso l'accesso ai dati ai sensi del presente accordo.
4. Ciascuna delle Parti nomina un proprio Referente Tecnico dell'esecuzione dell'accordo, responsabile dell'attivazione e della successiva gestione operativa dell'accesso ai dati, nonché della corretta applicazione delle regole di sicurezza tecnico-organizzative previste nell'accordo. I ruoli di Referente Tecnico

dell'esecuzione dell'accordo e di Responsabile dell'accordo possono essere ricoperti dalla stessa figura.

5. I nominativi ed i recapiti dei Referenti Tecnici sono riportati nell'allegato 2. Rientra nei compiti del Referente Tecnico:
  - a) garantire la verifica interna sull'adeguamento alle misure di sicurezza previste dal Codice, dalle Linee guida Agid citate in premessa e dal provvedimento del Garante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" del 2 luglio 2015;
  - b) comunicare tempestivamente all'altra Parte incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto nei processi di sicurezza afferenti la fruibilità dei dati oggetto dell'accordo;
  - c) comunicare tempestivamente all'altra Parte ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione online
  - d) garantire l'adeguamento delle misure di sicurezza ai progressi tecnologici e all'evoluzione dei rischi.
6. Inoltre, il Referente Tecnico dell'ente fruitore provvederà a:
  - a) adottare le procedure necessarie per la verifica sistematica e la revisione periodica delle abilitazioni e dei profili di accesso ai dati rilasciati, attraverso un adeguato flusso informativo con l'unità interna responsabile del trattamento;
  - b) adottare le procedure necessarie alla conservazione delle informazioni acquisite per il tempo strettamente necessario allo svolgimento delle attività per i cui dati sono stati acceduti e la loro distruzione quando le stesse non siano più necessarie;
  - c) curare le comunicazioni all'erogatore nei casi di eventuali errori o inesattezze e/o manchevolezze riscontrate in ordine ai dati acceduti.
7. Il Referente tecnico di Regione Lombardia provvederà a:
  - a) verificare di concerto con l'ente fruitore, la corretta attribuzione dei profili di autorizzazione;
  - b) redigere ed aggiornare un documento riportante l'indicazione delle banche dati accessibili, delle informazioni inerenti i soggetti fruitori e le informazioni relative al formato dei dati disponibili.
8. Nel caso di applicazioni web con attribuzione di credenziali individuali, Regione Lombardia ed Ente fruitore si accordano per una gestione delle utenze effettuata da Regione Lombardia, oppure per una gestione delle utenze diretta da parte dell'Ente fruitore.
9. Le figure previste nel processo di gestione delle credenziali di accesso sono quelle del Supervisore e dell'Amministratore Utenze. Vista l'architettura della

*web application* di fruizione sistema informativo del presente accordo, le due figure devono essere ricoperte da un unico soggetto, identificato nella *web application* con la figura di “Amministratore degli accessi”.

10. La nomina del soggetto Supervisore e Amministratore Utenze è sempre obbligatoria, sia presso il soggetto erogatore, sia presso l’Ente fruitore.

11. Il Supervisore ha il compito di:

- a) definire i profili di accesso;
- b) autorizzare le utenze che hanno accesso alla banca dati;
- c) vigilare sul corretto utilizzo degli accessi da parte degli utenti abilitati;
- d) autorizzare la revoca delle autorizzazioni al venir meno delle condizioni che ne hanno determinato la concessione;
- e) controllare l’attività dell’amministratore utenze, qualora il ruolo non sia da egli stesso ricoperto;
- f) revocare le autorizzazioni al venir meno delle condizioni che ne hanno determinato la concessione.

12. L’Amministratore utenze provvede a:

- a) effettuare la richiesta di assegnazione di credenziali di accesso per gli utenti;
- b) implementare le utenze per l’accesso alle banche dati;
- c) revocare le autorizzazioni al venir meno delle condizioni che ne hanno determinato la concessione.

13. Il nominativo e i recapiti del Supervisore/ Amministratore Utenze previsto dal presente accordo sono indicati nell’allegato 2.

## **ART. 5 – Modalità di accesso al Sistema integrato di sicurezza partecipata**

- 1. Regione Lombardia, tenuto conto della normativa vigente, fornisce all'ente fruitore l'accesso, in modalità *web-application* tramite service provider, ai dati presenti sulle piattaforme *social* per i quali l’utente ha espresso specifico consenso alla fruizione da parte di terzi in ottemperanza alle *policy* per le API adottate da ciascuna.
- 2. La modalità di accesso alle banche dati regionali più idonea sarà in ogni caso individuata da Regione LOMBARDIA tenendo conto delle finalità, della natura e della qualità dei dati, delle caratteristiche infrastrutturali e organizzative, del volume e della frequenza degli accessi, del numero di soggetti abilitati. Tale modalità sarà indicata in fase di richiesta di accesso alla specifica banca dati da parte dell’Ente fruitore, come da **allegato 4**.
- 3. L'accesso ai dati è consentito esclusivamente al personale riportato nell'**allegato 3** del presente accordo, espressamente incaricato del loro trattamento ed a ciò autorizzato nel rispetto delle norme vigenti e delle procedure tecniche ed



organizzative concordate con Regione Lombardia, dal Responsabile del trattamento dei dati dell'ente fruitore.

4. L'ente fruitore si impegna ad incaricare il minor numero possibile di personale. Eventuali richieste di superamento del numero di utenze autorizzate, deve essere concordata con l'erogatore per il tramite del responsabile dell'accordo. L'elenco del personale incaricato può variare a seguito di controlli effettuati da Regione Lombardia, o per variazioni organizzative dell'ente fruitore. A tal fine l'allegato 3 dovrà essere aggiornato a cura dei Responsabili dell'accordo.
5. Sono seguite specifiche procedure per la distribuzione sicura delle credenziali di autenticazione o, nei casi di utilizzo di forme di autenticazione forte, quali quelle che prevedono l'uso di one time password o di certificati di autenticazione, dei dispositivi necessari per abilitarla.

#### **ART. 6 – Titolarità e trattamento dei dati**

1. Regione Lombardia conserva la piena titolarità delle informazioni contenute nel Sistema Integrato di Sicurezza Partecipata (SISP), nonché degli applicativi utilizzati. L'ente fruitore assume il ruolo di autonomo ed esclusivo titolare del trattamento dei dati.
2. Le Parti rispettivamente si vincolano alla scrupolosa osservanza delle disposizioni del Codice, in particolare per quanto riguarda la sicurezza dei dati, gli adempimenti e la responsabilità nei confronti degli interessati, dei terzi e dell'Autorità del Garante per la protezione dei dati personali.
3. Ai sensi dell'art.11 del Codice, i dati trattati in applicazione del presente accordo dovranno essere pertinenti, completi e non eccedenti rispetto alle finalità perseguite dall'ente fruitore.
4. L'ente fruitore, in qualità di autonomo titolare, assicura che i dati personali acquisiti saranno trattati esclusivamente per le finalità previste nell'allegato 1. Assicura altresì che i dati medesimi non saranno divulgati, comunicati né ceduti a terzi, o riprodotti, al di fuori dei casi previsti dalla legge.
5. L'ente fruitore garantisce che l'accesso alle informazioni verrà consentito esclusivamente ai soggetti designati quali responsabili o incaricati del trattamento dei dati, impartendo ai sensi rispettivamente degli articoli 29 e 30 del Codice precise e dettagliate istruzioni, richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati, nonché al corretto utilizzo delle funzionalità dei collegamenti.

#### **ART. 7 – Tutela della sicurezza dei dati**

1. Ente fruitore e Regione Lombardia gestiscono i trattamenti dati di cui sono titolari nel rispetto delle misure di sicurezza di cui all'allegato B del Codice.

2. L'Ente fruitore e l'Ente erogatore si impegnano altresì a rispettare ulteriori misure tecniche ed organizzative derivanti dal provvedimento del Garante “Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche” del 2 luglio 2015, riportate in allegato 4 del presente accordo.
3. Regione Lombardia garantisce la corretta erogazione dei servizi di accesso ai dati previsti dal presente accordo e si impegna a verificare periodicamente che le informazioni saranno acquisite attraverso il Sistema Integrato di Sicurezza Partecipata (SISP) esclusivamente per le finalità dichiarate nell'accordo e in fase di richiesta di accesso, come da allegato 1, nel rispetto dei principi di pertinenza e non eccedenza, nonché di indispensabilità, per i dati sensibili e giudiziari.
4. L'Ente fruitore si impegna, inoltre, a comunicare tempestivamente qualsiasi incidente occorso che abbia impatto diretto o indiretto sulla sicurezza dei dati o sul sistema di autenticazione, nonché ogni modificazione tecnica e organizzativa che possa incidere sul contenuto del presente accordo. In particolare, si impegna a comunicare tempestivamente ogni mutamento avvenuto in ordine al personale autorizzato, alle modifiche tecniche o organizzative di dominio.

#### **ART. 8 – Tracciamento degli accessi e controlli**

1. L'Ente fruitore si impegna a comunicare ai propri incaricati che, in ottemperanza all'art 5, lettera m), del provvedimento del Garante “Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche” del 2 luglio 2015, le operazioni di accesso al viewer, di scaricamento del report e di accesso ad almeno un post vengono tracciate.
2. Tali registrazioni, in caso di violazione della normativa vigente, sono messe a disposizione dell'Autorità competente.
3. Le Parti svolgono congiuntamente attività di verifica consistenti nel monitoraggio degli accessi e delle transazioni effettuate dagli incaricati.
4. A fronte di eventuali anomalie riscontrate, l'ente fruitore consentirà anche verifiche puntuali sulla legittimità degli accessi, impegnandosi a fornire all'erogatore tutti i chiarimenti e la documentazione che si rendesse necessaria a seguito dell'attivazione dei controlli di cui trattasi.

#### **ART. 9 – Disposizioni finanziarie**

1. Ciascuna delle Parti si fa carico dei costi derivanti dall'attuazione dell'accordo.

2. Sono a carico di Regione Lombardia le spese per la realizzazione Sistema Integrato di Sicurezza Partecipata (SISP) e la sua fruibilità agli Enti sottoscrittori del presente Accordo.

#### **ART. 10 – Durata**

1. L'accordo ha effetto a decorrere dalla data di sottoscrizione da parte delle parti, fino al 31/12/2020.

#### **ART. 11 – Clausola di recesso**

1. La mancata ottemperanza ai vincoli di accesso ai dati ed il venir meno dei presupposti e dei requisiti di cui agli allegati al presente accordo costituiscono causa di recesso dalla stessa e di immediata sospensione dei servizi a seguito di formale comunicazione. Le Parti concordano che l'accordo trova inoltre immediata conclusione laddove vengano meno le finalità per le quali l'accesso ai dati è stato autorizzato.

#### **ART. 12 – Composizione dell'accordo**

1. L'accordo si compone di 12 articoli e di 5 allegati, relativi a:
  - allegato A: "Sistema integrato di sicurezza partecipata" - descrizione sistema;
  - allegato 1: Modulo di adesione Sistema integrato di sicurezza partecipata;
  - allegato 2: figure organizzative previste dall'accordo e loro recapiti di contatto;
  - allegato 3: elenco del personale dell'ente fruitore incaricato ad accedere alla Sistema integrato di sicurezza partecipata;
  - allegato 4: modalità di attivazione e fruizione dei servizi di accesso, misure di sicurezza tecniche.

**Sistema integrato di sicurezza partecipata** attraverso l'interrogazione del Cruscotto multidimensionale di monitoraggio per l'analisi e la consultazione delle segnalazioni di episodi di degrado e insicurezza urbana derivanti da fonti quali i social media ed i dati satellitari del territorio dell'Ente si ottiene un valido strumento di lavoro per il monitoraggio della sicurezza urbana nell'Ente.

### 1. Contesto

Il presente allegato descrive le caratteristiche delle informazioni previste per garantire il flusso operativo che attraverso l'integrazione dei dati provenienti dai social media e le rilevazioni satellitari "mirate" e "storicizzate" rendono possibile recuperare informazioni fornendo all'Ente locale uno strumento utile per definire le azioni di prevenzione e controllo sul territorio. L'utilizzo combinato dei dati social e satellitari, ove presenti, per finalità di sicurezza urbana rappresenta dal punto di vista metodologico e di progettazione del servizio un elemento indubbiamente innovativo.

### 2. Caratteristiche e descrizione del servizio

Punto di accesso: <https://sicurezza.servizirl.it/web/polizia-locale/cisp>

I dati sono acquisiti mediante l'analisi dei post pubblicati su blog e social media da cittadini comuni e da profili pubblici, di articoli di blog e di siti di testate giornalistiche. Sono sottoposti ad analisi i post pubblici su una serie di blog e piattaforme social, fra cui Facebook e Twitter. Gli attributi dei dati social rilevati attraverso l'utilizzo del servizio di estrazione e analisi dei dati sono:

- Data segnalazione
- Fonte
- Contenuto della segnalazione
- Georeferenziazione
- Parola chiave (abusivismo / rifiuti / criminalità / quiete pubblica)

I dati relativi alla georeferenziazione vengono individuati in base alla località nominata nel contenuto della segnalazione, non in base alla geolocalizzazione data dal luogo da cui viene pubblicata, che è ricompresa nel flusso.

Il sistema è dotato di una modalità di visualizzazione dei dati social che garantisce con visibilità diversificati in base all'utente che accede al servizio, in modo da consentire

solamente la visualizzazione dei post geolocalizzati nell'area territoriale di pertinenza dell'ente fruitore per il quale l'utente opera.

Il Sistema integrato di Sicurezza Partecipata SISP permette quindi di effettuare una raccolta di dati di segnalazioni di degrado e insicurezza urbana derivanti dalle piattaforme social per promuovere il costante monitoraggio dei fenomeni relativi a situazioni di criticità urbane.

Inoltre, il sistema si avvale anche di una collezione di immagini satellitari ad alta risoluzione di nuova e vecchia acquisizione che coprono il territorio di Milano e dei comuni della cintura milanese. Su queste immagini vengono effettuate delle analisi per monitorare il cambiamento nel tempo sul territorio in termini di abusivismo (edilizio ed ambientale).

Tali attività consentiranno di alimentare un cruscotto multidimensionale di monitoraggio attraverso il quale sarà possibile condurre l'analisi e la consultazione delle segnalazioni di degrado e insicurezza urbana.

I dati raccolti attraverso i social network saranno trattati per il raggiungimento delle finalità di cui sopra e verranno resi disponibili attraverso le seguenti macro-funzionalità:

- Disponibilità di *heatmap*, cioè delle mappe di calore in cui il colore rappresenta la concentrazione dei fenomeni osservati, sovrapposte alla mappa del luogo cui le segnalazioni si riferiscono. È disponibile la funzionalità di zoom per localizzare i luoghi per i quali le segnalazioni danno indicazioni puntuali.
- Accedere ovvero cliccare sulla URI corrispondente al post ed aprire sul browser il post principale direttamente sul social media (per quanto concerne Facebook, nel caso in cui il post selezionato sia un commento ad un post principale di una pagina pubblica, l'utente viene proiettato sul post principale e da lì può scorrere i commenti, ma non viene proiettato direttamente sul commento).

**Modulo di adesione al Sistema integrato di sicurezza partecipata**

Spettabile Regione Lombardia

PEC: .....

**Oggetto: Domanda di autorizzazione all'accesso al Sistema Integrato di Sicurezza Partecipata (SISP), oggetto dell'accordo per la fruibilità dei dati**

L'Ente \_\_\_\_\_ con sede in \_\_\_\_\_  
Codice Fiscale \_\_\_\_\_ indirizzo PEC \_\_\_\_\_  
legalmente rappresentato da \_\_\_\_\_, in qualità  
di \_\_\_\_\_

visto l'accordo per la fruibilità telematica delle banche dati di REGIONE e relativi allegati e valutati tutti gli adempimenti ivi previsti, **dichiara di aderire al seguente accordo in tutti i suoi elementi e richiede** l'accesso ai dati in elenco, contenuti nella seguente banca dati: **Sistema integrato di sicurezza partecipata**.

La base normativa che legittima l'Ente all'acquisizione dei dati e le finalità istituzionali perseguite con i dati raccolti, nel rispetto dei principi di pertinenza e non eccedenza del trattamento dei dati personali, è costituita:

- dalla legge n. 65/1986, che disciplina, tra l'altro, il conferimento delle qualifiche di polizia giudiziaria e di agente di pubblica sicurezza, nonché l'accessoria qualifica, per tutti gli operatori di polizia giudiziaria, di agenti accertatori di polizia amministrativa (art. 13 della L. 689/1981);
- dalla L.R. 6/2015 e ss.mm.ii., per le seguenti finalità istituzionali: ex art. 3 (Politiche integrate di sicurezza urbana), comma 1, lettera c): promozione da parte di Regione Lombardia dello scambio di informazioni e dati con gli organi dello Stato e con altri enti pubblici locali per la conoscenza dei fenomeni criminali e delle situazioni di degrado presenti sul territorio regionale.

La sussistenza del rispetto di tali presupposti sarà soggetta a preventiva verifica.

*Data e luogo*

\_\_\_\_\_

*Firma e timbro del Legale Rappresentante*

\_\_\_\_\_

**Figure organizzative previste dall'accordo e loro recapiti di contatto**

Le figure di riferimento per l'**ente fruitore** sono:

***Responsabile dell'accordo:***

*Nominativo* .....

*Telefono* .....

*E mail* .....

*C.F.* .....

***Referente tecnico dell'esecuzione dell'accordo:***

*Nominativo* .....

*Telefono* .....

*E mail* .....

*C.F.* .....

***Amministratore utenze e Supervisore:***

*Nominativo* .....

*Telefono* .....

*E mail* .....

*C.F.* .....

Le figure di riferimento per **Regione Lombardia** sono:

***Responsabile dell'accordo:***

*Nominativo* .....

*Telefono* .....

*E mail:* .....

*C.F.* .....

***Referente tecnico dell'esecuzione dell'accordo:***

*Nominativo .....*

*Telefono .....*

*E mail: .....*

*C. F. ....*



**Elenco del personale dell'ente fruitore incaricato ad accedere al Sistema integrato di sicurezza partecipata**

Al fine della stipulazione dell'Accordo l'Ente fruitore dichiara che:

Il numero delle utenze che si prevede di abilitare è pari a: .....

Il personale autorizzato è il seguente:

<b>Nominativo</b>	<b>Codice fiscale</b>	<b>Profilo d'accesso</b>
		Legale Rappresentante
		Amministratore degli accessi
		Operatore
		Operatore
		Operatore

## **Modalità di attivazione e fruizione dei servizi di accesso, misure di sicurezza tecniche.**

### **Art. 1 – Modalità di fruizione Sistema integrato di sicurezza partecipata**

1. L'accesso alla banca dati è fornito col seguente profilo di utilizzo orario:

- orario continuato 7x24

2. L'accesso alla banca dati avviene con le seguenti modalità:

- *Web-Application collegandosi al Portale dei Servizi della Direzione Sicurezza*

*(<https://sicurezza.servizirl.it/>)*

### **Art. 2 – Misure di sicurezza tecniche**

Le misure adottate da Regione Lombardia e sotto riportate rappresentano il riferimento alla *best practice* indirizzata dal provvedimento del Garante del 2 Luglio 2015, suddivise in funzione del tipo di accesso prescelto.

Ulteriori misure, oltre a quelle qui elencate possono essere eventualmente introdotte al fine di meglio salvaguardare la sicurezza dei propri sistemi e dei dati trattati, dopo che siano stati individuati e valutati rischi particolari derivanti dalla rilevanza delle informazioni accedute, delle dimensioni della banca dati, del numero degli utenti, o del volume dei trasferimenti. A titolo esemplificativo:

- Modalità di accesso con *strong authentication*
- Periodo di conservazione non superiore ai due mesi per i post, passando poi alla trasformazione in dati anonimi o alla trasformazione in dati statistici cumulativi.
- Minimizzazione e anonimizzazione: i riferimenti agli account facebook e twitter dei “privati cittadini” sono eliminati dal flusso già all’atto dell’acquisizione, prima dello inserimento nella banca dati.
- Avviso di navigazione fuori dall’applicativo regionale all’atto di ogni “click” su una singola segnalazione.
- Tracciamento applicativo delle attività (login/logout e click su URI dei post) per consentire verifiche su eventuale illecito utilizzo da parte di uno e più utenti ;

Analogamente, le misure di sicurezza per la protezione dei dati personali nello scambio fra PA possono trovare diversa applicazione e modulazione qualora, a seguito di analisi dei flussi in ottica *risk based*, siano emerse motivazioni documentate tali da giustificarlo.

**a) Misure applicabili per accessi via *web application***

1. L'ente fruitore accede alle banche dati per mezzo di postazioni di lavoro connesse alla rete internet con precauzioni di sicurezza adeguate e gestite dall'ente in autonomia, rendendo quindi esente ARIA e Regione da eventuali problemi di sicurezza rilevati sul *client*.
2. È consentita all'ente fruitore l'estrazione **unicamente dei dati di propria competenza**, per via automatica e massiva, anche con lo scopo di replicare gli stessi su autonome banche dati; in questo caso ARIA viene esentata da qualsivoglia responsabilità in ordine alla diffusione di tali dati.