



Comune
di Molinella

Città Metropolitana di Bologna

COMUNE DI MOLINELLA

**DATA PROTECTION IMPACT
ASSESSMENT (DPIA)
VALUTAZIONE D'IMPATTO**

**SISTEMA AEROMOBILE "SAPR"
(DRONE) - UAS**

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

SISTEMI AEROMOBILI A PILOTAGGIO REMOTO (SAPR - DRONI)

Ente: Comune di Molinella

Titolare del Trattamento: Sindaco p.t. Bruno Bernardi

Responsabile Interno del Trattamento: Dott. Giuliano Corso (Comandante PL)

Data Protection Officer (DPO): Gloriamaria Paci (Studio Paci Srl)

1. Contesto e Finalità del Trattamento

La presente valutazione d'impatto, redatta ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (GDPR) e del D.Lgs. 51/2018, analizza i trattamenti di dati personali derivanti dall'impiego di droni in dotazione alla Polizia Locale.

- **Finalità:** Polizia giudiziaria, monitoraggio ambientale (es. sversamenti abusivi), rilevamento sinistri stradali complessi, supporto alla protezione civile e sicurezza urbana.
- **Basi giuridiche:** Esecuzione di un compito di interesse pubblico (GDPR) e finalità di prevenzione e indagine di reati (D.Lgs. 51/2018).

2. Necessità e Proporzionalità

L'uso dei droni si rende necessario in quanto gli strumenti ordinari (telecamere fisse o bodycam) non consentono una visione d'insieme in scenari complessi, impervi o ad alto rischio. La proporzionalità è garantita dall'utilizzo "on demand" del dispositivo: il volo non è sistematico, ma attivato solo al verificarsi di specifici eventi o su delega dell'Autorità Giudiziaria. Il sorvolo di aree private o non pertinenti è vietato, salvo necessità investigative urgenti.

3. Analisi e Valutazione dei Rischi

Minaccia / Rischio	Impatto	Misure di Mitigazione Adottate	Rischio Residuo
Registrazione accidentale di soggetti estranei alle indagini / aree private	Alto	Pianificazione rigorosa del piano di volo (geofencing). Attivazione ripresa solo sull'obiettivo. Segnaletica nell'area	Medio

Minaccia / Rischio	Impatto	Misure di Mitigazione Adottate	Rischio Residuo
		di decollo.	
Accesso non autorizzato ai dati archiviati (Data Breach)	Alto	I dati risiedono su schede SD cifrate a bordo del drone e vengono scaricati su server in rete segregata con accesso tramite credenziali forti.	Basso
Intercettazione del flusso video durante il volo (Sniffing)	Medio	Protocolli di trasmissione radio crittografati tra drone e radiocomando. Assenza di streaming su cloud pubblici.	Basso
Smarrimento o furto del SAPR con a bordo i dati	Medio	Cifratura hardware dei supporti di memoria a bordo (es. AES-256). Formattazione periodica dopo il travaso dei dati.	Basso

4. Conservazione dei Dati (Data Retention)

I dati registrati dal SAPR vengono conservati per un periodo massimo di **7 giorni**. Il prolungamento di tale periodo è ammesso esclusivamente nel caso in cui i filmati costituiscano prova in un procedimento penale o amministrativo (fino a conclusione dell'iter) o su specifica richiesta dell'Autorità Giudiziaria.

5. Conclusioni e Parere del DPO

A seguito dell'analisi, tenuto conto delle finalità di sicurezza urbana e delle forti misure tecniche ed organizzative implementate (disciplinare interno, cifratura, segregazione reti), si valuta che i rischi per i diritti e le libertà degli interessati siano mitigati a un livello accettabile. Non si ritiene necessaria la consultazione preventiva del Garante ex art. 36 GDPR.