COMPLIANCE BRIEFING #014 · 29 MAGGIO 2026

Sanzioni del Garante Privacy 2020-2026: 10 casi che fanno scuola per chi opera con drone e videosorveglianza

Dal 2020 a oggi il Garante per la protezione dei dati personali ha applicato sanzioni che cambiano il modo in cui un operatore UAS deve pensare alla privacy. Dieci provvedimenti — da TIM €27,8M del 2020 alle istruttorie contro Bari/Roma Capitale/ASL Roma 3 sul Covid (settembre 2021) fino a Realmaps €100K del 2025 — raccontano dove sta la linea che il Garante traccia tra videosorveglianza compliant e non. Gli errori che il Garante sanziona nei casi statici (Mark Bologna, Recco, Castel Goffredo) sono gli stessi che farà un operatore UAS che monti payload video senza ROPA, DPIA, informativa, art. 28. Il drone non è caso speciale: è una telecamera che si muove. Tutti i provvedimenti citati hanno doc web verificato sul portale Garante.

Sanzioni del Garante Privacy 2020-2026: 10 casi che fanno scuola per chi opera con drone e videosorveglianza

Settembre 2021. Il Garante per la protezione dei dati personali apre tre istruttorie nello stesso giorno: Comune di Bari, Roma Capitale, ASL Roma 3 (doc web 9696781). Vogliono usare i droni — per assembramenti, per discariche abusive, per misurare la febbre sulla spiaggia di Ostia. Il Garante chiede a tutti la stessa cosa: dove sta la DPIA?

Da quel momento in poi, ogni operatore UAS che monta una camera ha un benchmark istruttorio sopra la testa. Dal 2020 a oggi, dieci provvedimenti raccontano dove sta la linea — e dove finisce l'attività di un titolare del trattamento che pensava di "usare un drone come fa il vicino di casa". Questo articolo li mette in fila.

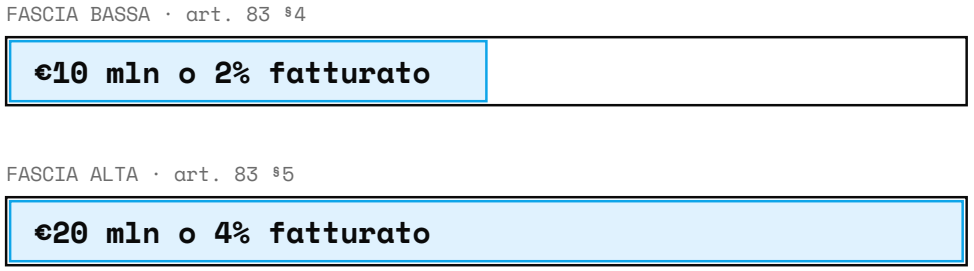
La tesi è semplice: gli errori che il Garante sanziona nelle videosorveglianze statiche (Mark Bologna, Recco, Castel Goffredo) sono gli stessi che farà un operatore UAS che monti payload video senza ROPA, senza DPIA, senza informativa, senza nomina art. 28. Il drone non è caso speciale: è una telecamera che si muove. Le regole della videosorveglianza si applicano per intero — più qualcosa.

Tutti i provvedimenti citati hanno doc web verificato sul portale Garante. La guida è complemento naturale di CB#007 DPIA drone: dai casi (CB#014) alla procedura preventiva (CB#007).

> Disclaimer: alcuni provvedimenti citati (tra cui Enel Energia 19/1/2022) sono stati impugnati in sede giudiziaria e annullati in primo grado. Le decisioni del Garante non sono "definitive" fino all'esaurimento dei gradi di giudizio. Questa guida cita i provvedimenti per il loro valore di benchmark interpretativo (cosa il Garante considera errore), non come oracolo definitivo del rischio.

---

01 Quadro normativo — i massimali GDPR e i criteri di ponderazione



SCHEMA — I DUE MASSIMALI GDPR (SI APPLICA IL MAGGIORE TRA IMPORTO E % FATTURATO)

Le sanzioni amministrative del Garante poggiano su due livelli:

Quadro UE — GDPR art. 83

L'art. 83 par. 4 GDPR prevede sanzioni "fascia bassa": fino a €10 milioni o 2% del fatturato annuo mondiale (il maggiore tra i due). Si applica a violazioni di obblighi del titolare/responsabile — artt. 8, 11, 25-39 (privacy by design, ROPA, DPO, DPIA), 42, 43.

L'art. 83 par. 5 GDPR prevede sanzioni "fascia alta": fino a €20 milioni o 4% del fatturato annuo mondiale. Si applica a violazioni dei principi (art. 5), basi giuridiche (art. 6, 9), diritti dell'interessato (artt. 12-22), trasferimenti extra-UE.

L'art. 83 par. 2 GDPR elenca 11 criteri di ponderazione obbligatori che il Garante deve considerare nel calibrare la sanzione concreta: natura/gravità/durata, intenzionalità o negligenza, misure di mitigazione adottate, grado di responsabilità, precedenti, cooperazione con l'autorità, categorie di dati, modalità di scoperta del fatto, aderenza a codici di condotta, benefici economici tratti.

Quadro italiano — Codice Privacy

- Art. 166 Cod. Privacy (D.Lgs. 196/2003 mod. D.Lgs. 101/2018) — criteri applicativi delle sanzioni amministrative + procedimento (rinvio a L. 689/1981 per parti non disciplinate da GDPR)
- Art. 167 Cod. Privacy — illeciti penali: trattamento dati per trarre profitto a danno dell'interessato → reclusione fino a 6 anni se categorie particolari (art. 9 GDPR)
- Art. 2-ter Cod. Privacy — base giuridica del trattamento dati personali da parte di pubblici poteri (norma di legge o regolamento). Centrale per i casi PA citati sotto
- Art. 114 Cod. Privacy — garanzie lavoratori (rinvio art. 4 Statuto Lavoratori L. 300/1970) → autorizzazione preventiva ITL per videosorveglianza in luoghi di lavoro

Fonte interpretativa primaria

Tutti i provvedimenti del Garante in materia video richiamano sistematicamente le Linee Guida 3/2019 v2.0 dell'EDPB sul trattamento di dati personali attraverso dispositivi video (adottate 29 gennaio 2020). Per chi opera con drone, queste linee guida sono la fonte interpretativa di riferimento per capire come il Garante leggerà il vostro caso.

---

02 Come decide il Garante — i criteri art. 83 par. 2

I 11 criteri di ponderazione del par. 2 GDPR si applicano in modo cumulativo. Nel calibrare la sanzione concreta, il Garante valuta:

- Natura, gravità, durata della violazione
- Intenzionalità o negligenza (dolo aumenta, "buona fede" riduce)
- Misure di mitigazione adottate dopo aver scoperto la violazione
- Grado di responsabilità del titolare alla luce delle misure tecniche e organizzative
- Eventuali precedenti violazioni pertinenti del titolare
- Cooperazione con l'autorità per porre rimedio
- Categorie di dati interessati (art. 9 → aggravante)

- Modalità di scoperta del fatto (segnalazione interessato, audit, denuncia)
- Aderenza a codici di condotta o meccanismi di certificazione
- Benefici economici ottenuti dalla violazione
- Altri elementi: dimensione del soggetto, fatturato, gravità del danno

In pratica: stesso fatto = sanzioni molto diverse a seconda di quanto cooperate, di quanto vi mostrate ravveduti, di quanto la PA o l'impresa abbia documentato il proprio iter compliance ex ante.

---

03 Le sanzioni-record — quadro macro

Per dare l'idea dell'ordine di grandezza in cui il Garante si muove, tre sanzioni "record" che funzionano da benchmark per qualsiasi caso minore.

Data	Soggetto	Sanzione	Fatti chiave
1/2/2020	TIM S.p.A. (doc web 9256409)	€27.802.946	Marketing illecito (milioni di chiamate senza consenso), gestione data breach inadeguata, privacy by design assente. Violazioni artt. 5, 6, 7, 17, 21, 24, 25, 32 GDPR
19/1/2022	Enel Energia (doc web 9737661)	€26.513.977 (annullata in primo grado dal Trib. Roma, appello pendente)	Telemarketing aggressivo, no consenso, opt-out ignorati, accountability assente. Artt. 5, 6, 7, 24
17/4/2024	Enel Energia (sanzione record assoluta nel 2024)	€79 milioni	Condotte sistemiche di violazione su data subjects multipli

Questi importi non sono pensati per gli operatori UAS (le compagnie energetiche italiane hanno fatturati nell'ordine dei miliardi). Servono come benchmark concettuale: il Garante può applicare massimali milionari quando trova condotte sistemiche e accountability assente. Per i casi UAS-rilevanti, gli importi sono tipicamente più contenuti — ma il pattern degli errori contestati è lo stesso.

---

04 I 10 casi che fanno scuola per chi opera con drone

Selezione di provvedimenti 2020-2026 con doc web verificato sul portale Garante. Sono i casi più rilevanti per un operatore UAS perché coprono:

- Uso effettivo di droni (Treviso 2024, istruttorie Covid 2021)
- Videosorveglianza statica con dinamiche identiche al drone (Mark Bologna, Recco, Castel Goffredo)
- Errori procedurali sistemici che si applicano per analogia (Realmaps, ARSAC)

#	Data	Soggetto	Doc web	Fatti chiave	Sanzione
1	1/2/2020	TIM S.p.A.	9256409	Marketing illecito + breach gestione + no privacy by design	€27.802.946
2	3/9/2021	Comune Bari + Roma Capitale + ASL Roma 3	9696781	Istruttorie su uso droni Covid (assembramenti, illeciti ambientali, misurazione febbre Ostia) — richiesta DPIA, base giuridica, retention	Istruttorio (no sanzione finale pubblica)
3	19/1/2022	Enel Energia	9737661	Telemarketing aggressivo	€26.513.977 (annullata Trib. Roma, in appello)
4	16/11/2023	Comune di Castel Goffredo (MN)	9963486	Telecamera audio-video presso Comando Polizia Locale senza autorizzazione art. 4 L. 300/70; comunicazione illecita registrazione	€50.000
5	4/7/2024	Comune di Treviso	10050298	App "TrevisoSicura" + uso droni con telecamere termiche — segnalazioni cittadine reati senza informativa adeguata, no DPA con fornitore, ruoli art. 28 errati. Droni archiviati per dichiarata non identificazione	€7.000 (per app)
6	17/7/2024	Mark s.r.l.s. — "The Lull Bar" (BO)	10070348	10 telecamere senza cartellonistica + no	€5.000

#	Data	Soggetto	Doc web	Fatti chiave	Sanzione
				autorizzazione ITL preventiva, installazione sanata ex post	
7	16/1/2025	Realmaps S.r.l.	10110241	Liste proprietari immobili a agenzie senza consensi, no DPIA, no DPO, no ROPA, art. 28 omessi	€100.000
8	13/3/2025	ARSAC (Reg. Calabria)	10128005	Geolocalizzazione GPS dipendenti smartworking via app "Time Relax", uso disciplinare dei dati	Dichiarazione di illiceità + pubblicazione; no sanzione (ente aveva cessato)
9	4/6/2025	Comune di Recco (GE)	10163530	Videosorveglianza fissa OCR su conferimento rifiuti senza cartellonistica primo livello	€5.000
10	11/9/2025	Caso videosorveglianza condominiale post-Linee Guida 209/2025	10183820	Telecamere ad angolo eccedente aree comuni, no delibera assembleare art. 1122-ter c.c., no ROPA	Da approfondire

---

05 Pattern degli errori — cosa si ripete in 8 casi su 10

Analizzando i provvedimenti, lo stesso errore si ripete in modo statistico significativo:

Errore	Frequenza	Riferimento normativo	Esempi
Informativa assente o inadeguata (art. 13 GDPR)	7/10	Art. 13 GDPR + EDPB GL 3/2019	Treviso, Recco, Mark Bologna, Castel Goffredo, Realmaps
Base giuridica non specificata o errata (art. 6 GDPR)	6/10	Art. 6 GDPR + art. 2-ter Cod. Privacy per PA	Treviso, istruttorie 2021, ARSAC, Realmaps

Errore	Frequenza	Riferimento normativo	Esempi
DPIA omessa (art. 35 GDPR)	5/10	Art. 35 GDPR + Provv. Garante 467/2018	Treviso, ARSAC, Realmaps, istruttorie 2021
ROPA assente o incompleto (art. 30 GDPR)	4/10	Art. 30 GDPR	Realmaps, condominio 2025
Nomina art. 28 omessa o sbagliata (responsabile esterno)	3/10	Art. 28 GDPR	Treviso (fornitore app), Realmaps
Privacy by design / default ignorati (art. 25)	5/10	Art. 25 GDPR	TIM, Treviso, Realmaps, ARSAC
Conservazione eccessiva (art. 5(1)(e))	3/10	Art. 5(1)(e) GDPR	Castel Goffredo, TIM
Comunicazione illecita a terzi (art. 6 par. 4)	2/10	Art. 6 par. 4 GDPR	Castel Goffredo, Realmaps
Mancato rispetto art. 4 L. 300/70 (lavoratori)	2/10	Art. 4 Statuto Lavoratori + art. 114 Cod. Privacy	Mark Bologna, Castel Goffredo

Lettura per UAS: il drone con payload video tipicamente accumula 4-5 di questi errori contemporaneamente se non c'è un setup compliance ex ante. Il caso Treviso 2024 è particolarmente istruttivo perché è una PA con DPO designato che comunque becca €7.000 per cumulo di errori procedurali — non per malafede. La designazione del DPO non è scriminante.

5.1 Cosa dice testualmente il Garante

Quattro passaggi letterali dai provvedimenti più rilevanti per UAS — utili per capire come pensa il Garante quando legge un trattamento video.

Comune di Treviso (doc web 10050298, 4/7/2024) — sul drone con termocamera:

> *"l'impiego di droni dotati di telecamere termiche, al fine di generare c.d. mappe di calore, sulla base delle quali possono essere disposti controlli de visu da parte delle pattuglie della Polizia locale in servizio sul territorio, può comportare un trattamento di dati personali (cfr. artt. 2, par. 1, e 4 nn. 1 e 2, del Regolamento), anche relativi a reati (v. art. 10 del Regolamento e 2-octies del Codice). [...] sebbene non sia possibile riconoscere il volto dei soggetti ripresi, le immagini permettono comunque di visualizzare, con un discreto livello di definizione, le sagome e i*

> *movimenti degli stessi. Si tratta, pertanto, comunque di informazioni che [...] possono essere associate a persone fisiche identificate ed essere utilizzate come elementi di prova di fattispecie di reato."*

Significa: anche le immagini termiche che non mostrano il volto sono dato personale se contestualizzate. Per UAS è il colpo letale al "tanto non si vedono i volti".

Comune di Treviso (stesso provvedimento) — sull'art. 28 omesso col fornitore dell'app:

> *"laddove [...] sussista 'un rapporto titolare-responsabile del trattamento [...] anche in assenza di un [valido] accordo di trattamento per iscritto' — in quanto il soggetto che tratta i dati effettua in concreto il trattamento non per proprie finalità ma per conto del soggetto committente e titolare del trattamento [...] — ciò implica una violazione dell'articolo 28, paragrafo 3, del [Regolamento]"* (cit. Linee guida EDPB 07/2020 par. 103).

Significa: la mancanza dell'accordo art. 28 GDPR per iscritto è violazione autonoma, indipendentemente dal fatto che il fornitore tratti correttamente.

Comune di Recco (doc web 10163530, 4/6/2025) — sul "legittimo interesse" delle PA:

> *"il legittimo interesse, ai sensi dell'art. 6, paragrafo 1, lett. f), del Regolamento, non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti"* (richiamato cons. 47 GDPR).

Significa: una PA non può mai giustificare un trattamento video richiamando "legittimo interesse" — serve sempre norma di legge/regolamento ex art. 2-ter Cod. Privacy.

Realmaps S.r.l. (doc web 10110241, 16/1/2025) — sulla DPIA non come formalità:

> *"il titolare del trattamento avrebbe dovuto effettuare, prima di iniziare il trattamento, una valutazione d'impatto [...] in considerazione, anche, della tipologia di dati trattati (informazioni anche di natura particolare) e del numero elevato di interessati coinvolti."*

Significa: prima di iniziare, non "ex post quando arriva l'istruttoria". Il timing della DPIA è esso stesso oggetto di sanzione.

---

06 Conseguenze pratiche — oltre la sanzione

La sanzione amministrativa pecuniaria è solo uno degli strumenti. Il Garante dispone di altre misure ex art. 58 par. 2 GDPR che spesso hanno impatto operativo maggiore della multa:

Strumento	Norma	Effetto
Ingiunzione di conformità	Art. 58 par. 2 lett. d	Ordine di rendere conforme il trattamento entro un termine
Divieto di trattamento	Art. 58 par. 2 lett. f	Blocco dell'attività di trattamento (impatto massimo)
Limitazione temporanea o definitiva	Art. 58 par. 2 lett. f	Limitazione di alcune finalità di trattamento
Dichiarazione di illiceità senza sanzione monetaria	Prassi	Caso ARSAC 13/3/2025: l'ente aveva già disattivato il trattamento → dichiarazione di illiceità + pubblicazione, no sanzione
Ammonimento (sanzione non pecuniaria)	Art. 58 par. 2 lett. b	Caso Liceo "Duca degli Abruzzi" Treviso (doc web 10039592, 4/7/2024 reg. provv. n. 403): trattamento illecito di dati Covid (categorie particolari art. 9), ma violazione minore ex cons. 148 GDPR → solo ammonimento. Esiste, è usato, e va a fascicolo (rilevante in caso di recidiva — art. 83 par. 2 lett. e)

Inoltre: danno reputazionale (i provvedimenti del Garante sono pubblicati e indicizzati dai motori di ricerca → cliente futuro che fa due'diligence li trova), azione civile da interessati ex art. 82 GDPR (risarcimento danno, anche non patrimoniale), e — in casi gravi — profilo penale ex art. 167 Cod. Privacy.

Per un operatore UAS commerciale, l'ingiunzione di conformità + divieto di trattamento può significare la sospensione delle operazioni in attesa di adeguamento.

---

07 Le 5 trappole comuni dedotte dai casi

Trappola 1 — "Tanto c'è il cartello"

Falso. I casi Mark Bologna e Recco dimostrano che il cartello *senza* informativa di secondo livello e *senza* contenuti minimi EDPB (titolare, finalità, base giuridica, contatti DPO, durata, diritti) non basta. Cartello generico = informativa assente. Per UAS, applicare il modello a due livelli EDPB GL 3/2019 §§ 109-122 (vedi CB#007).

Trappola 2 — "È PA, lavora in interesse pubblico"

Falso. Treviso, Castel Goffredo, ARSAC e le istruttorie 2021 dimostrano che la PA deve comunque dimostrare:

- Base giuridica ex art. 2-ter Cod. Privacy (norma di legge o regolamento)
- DPIA preventiva quando ricorrono i requisiti art. 35 GDPR

L'interesse pubblico non è autoesecutivo. Una delibera comunale di adozione del servizio drone non equivale a base giuridica di trattamento dati.

Trappola 3 — "Drone emergenziale Covid, la deroga ENAC copre tutto"

Falso. Le istruttorie 2021 lo smentiscono frontalmente. La deroga aeronautica ENAC autorizza il volo (rispetto alle regole UAS), non il trattamento dati. GDPR rimane in piedi: DPIA + base giuridica + retention restano obbligatori. Il Garante ha aperto istruttorie contro Comune Bari + Roma Capitale + ASL Roma 3 proprio perché stavano usando droni con normativa aeronautica emergenziale ma senza adempimenti privacy.

Trappola 4 — "Cancello le immagini dopo"

Falso. TIM e Castel Goffredo sono stati sanzionati anche per conservazione "eccessiva" ex art. 5(1)(e) GDPR — anche quando poi le immagini vengono cancellate. Conta la policy ex ante documentata nel ROPA: 24-72 ore salvo eventi, retention scritta, cancellazione automatica. La deletion a posteriori non sana la mancanza di policy.

Trappola 5 — "Il fornitore del software/app si occupa lui della privacy"

Falso. Caso Treviso è didattico: il Comune ha messo in piedi l'app "TrevisoSicura" senza DPA con il fornitore e con ruoli art. 28 errati. Per UAS commerciale: chi usa software third-party di flight planning + storage cloud delle immagini (DJI Cloud, FlightHub, ecc.) deve:

- Stipulare DPA art. 28 GDPR con il fornitore, per iscritto
- Mappare il fornitore come responsabile del trattamento nel ROPA
- Verificare che il fornitore abbia DPO e misure tecniche adeguate (art. 28 par. 1)

---

08 Checklist preventiva — 10 punti per non finire nei 10 casi

Pensata come complemento operativo alla checklist DPIA di CB#007.

- ☐ 1. ROPA aziendale art. 30 con voce dedicata "Riprese aeree UAS" (finalità, base giuridica, durata conservazione, categorie interessati, destinatari)
- ☐ 2. DPIA preventiva (art. 35) quando ricorrono i tre trigger art. 35 par. 3 o ≥ 2 criteri WP248
- ☐ 3. Base giuridica documentata (art. 6) — per UAS commerciale tipicamente 6(1)(b) contratto o 6(1)(f) legittimo interesse con test di bilanciamento scritto
- ☐ 4. Informativa primo livello — cartello area di volo con titolare + finalità + QR a informativa estesa
- ☐ 5. Informativa secondo livello — pagina web accessibile con tutti i contenuti EDPB GL 3/2019 §§ 109-122
- ☐ 6. DPA art. 28 con ogni fornitore esterno: cloud storage immagini, software flight log, fornitore drone con telemetria che esce verso cloud
- ☐ 7. Nomina art. 29 del pilota e dei dipendenti che visualizzano/elaborano le riprese
- ☐ 8. Retention policy scritta — di norma 24-72h salvo evento, documentata nel ROPA, cancellazione automatica
- ☐ 9. Privacy by design (art. 25) — blur targhe/volti in post-processing se non strettamente necessari, risoluzione minima utile, crittografia storage
- ☐ 10. Procedura diritti interessato (artt. 12-22) — modulo accesso, opposizione, cancellazione; tempi di riscontro entro 30 giorni

Aggiunte specifiche per operazioni in luoghi di lavoro: art. 114 Cod. Privacy + art. 4 L. 300/1970 → accordo sindacale o autorizzazione ITL prima del volo.

---

09 Come Hovra previene gli errori dei 10 casi

Hovra Own integra nel flusso missione i template e i workflow che evitano il pattern di errori contestati nei 10 casi del Garante:

- Threshold assessment automatico: per ogni pianificazione missione, l'app applica i 9 criteri WP248 e segnala se serve DPIA (evita il pattern errore "DPIA omessa" — 5/10 casi)
- Template ROPA strutturato: voce "Riprese aeree UAS" pre-compilata con tutti i campi art. 30 (evita "ROPA assente" — 4/10 casi)
- Generator informativa a due livelli: cartello primo livello + pagina web seconda livello editabile (evita "informativa inadeguata" — 7/10 casi)
- Template DPA art. 28 per fornitori standard del settore (DJI Cloud, FlightHub, AWS, ecc.) (evita "art. 28 omessi" — 3/10 casi)

- Test di bilanciamento legittimo interesse: workflow guidato per documentare per iscritto il test EDPB GL 3/2019 §§ 30-40 (evita "base giuridica errata" — 6/10 casi)
- Retention policy enforcer: cancellazione automatica dei raw dopo finestra configurabile + log della cancellazione (evita "conservazione eccessiva" — 3/10 casi)

→ Scopri il modulo Privacy Compliance su hovra.it → Articoli correlati: CB#003 Patentino A2/STS · CB#006 U-Space Italia 2026 · CB#007 DPIA drone

---

10 Bibliografia

Fonti normative

- Regolamento (UE) 2016/679 (GDPR). Art. 5, 6, 9, 13-14, 25, 28, 30, 35, 58, 82, 83 (sanzioni). EUR-Lex
- D.Lgs. 30 giugno 2003 n. 196 (Codice Privacy) modificato da D.Lgs. 101/2018. Normattiva. Artt. 2-ter (base giuridica PA), 114 (lavoratori), 166-167 (sanzioni amm. e penali)
- L. 20 maggio 1970 n. 300 (Statuto dei Lavoratori) art. 4 — controlli a distanza dei lavoratori
- L. 24 novembre 1981 n. 689 — Modifiche al sistema penale: procedimento sanzionatorio amministrativo

Fonte interpretativa primaria

- EDPB Linee Guida 3/2019 v2.0 sul trattamento di dati personali attraverso dispositivi video. Adottate 29 gennaio 2020. EDPB. Citate sistematicamente da tutti i provvedimenti Garante in materia video

Provvedimenti Garante citati (10 casi)

Data	Soggetto	Doc web
1/2/2020	TIM S.p.A.	9256409
3/9/2021	Bari + Roma Capitale + ASL Roma 3	9696781
19/1/2022	Enel Energia	9737661
16/11/2023	Comune Castel Goffredo	9963486
4/7/2024	Comune di Treviso (TrevisoSicura + droni) — reg. provv. n. 405	10050298

Data	Soggetto	Doc web
4/7/2024	*Bonus*: Liceo "Duca degli Abruzzi" Treviso (caso Covid+, ammonimento) — reg. provv. n. 403	10039592
17/7/2024	Mark s.r.l.s. (Bologna)	10070348
16/1/2025	Realmaps S.r.l.	10110241
13/3/2025	ARSAC (Calabria)	10128005
4/6/2025	Comune di Recco	10163530
11/9/2025	Condominio post-Linee Guida 209/2025	10183820

Articoli correlati nella serie

- CB#003 — Patentino A2 e STS — il pilota A2/STS è "responsabile del trattamento" *de facto* quando opera per terzi
- CB#006 — U-Space Italia 2026 — dati Network ID (posizione operatore) sono dati personali del pilota
- CB#007 — DPIA per drone — complemento naturale: dai casi (CB#014) alla procedura preventiva (CB#007)

Questo documento ha finalità informative e divulgative. I provvedimenti del Garante sono citati come benchmark interpretativo: alcuni sono stati impugnati e potrebbero essere annullati nei gradi successivi di giudizio. Per il caso concreto, consultare un DPO o un legale specializzato in privacy.

Nimber S.r.l.