

DPIA per operazioni con drone in Italia: quando è obbligatoria, come si fa, le sanzioni Garante 2020-2026

La DPIA (Data Protection Impact Assessment, art. 35 GDPR) è il primo errore di compliance privacy che un operatore UAS può fare — perché spesso non sa neppure se la deve fare. Per molte operazioni non scatta; per una minoranza significativa scatta e nessuno l'ha fatta. La guida sistematizza il quadro normativo (GDPR + Codice Privacy + Provv. Garante 467/2018 + EDPB GL 3/2019), le sei configurazioni tipiche dell'audience UAS, i casi Garante 2020-2026 verificati con doc web (Treviso 2024, Mark Bologna 2024, Castel Goffredo 2023, Realmaps 2025, istruttorie Bari/Roma/ASL Roma 3 2021), e il workflow operativo per fare DPIA, ROPA, informativa, art. 28 in modo coerente con la natura mobile del drone.

DPIA per operazioni con drone in Italia: quando è obbligatoria, come si fa, le sanzioni Garante 2020-2026

Il 4 luglio 2024 il Garante per la protezione dei dati personali ha archiviato il procedimento contro il Comune di Treviso per l'impiego di droni con telecamere termiche — ma solo perché l'ente ha dichiarato di non aver mai identificato persone. Nello stesso provvedimento ([doc web 10050298](#)), per altri trattamenti collegati (app "TrevisoSicura"), il Garante ha comminato €7.000 per omessa valutazione d'impatto e violazione degli artt. 5, 6, 13, 25, 28 GDPR.

Il messaggio per un operatore UAS è preciso: il primo errore di compliance privacy non è non avere la DPIA — è non sapere se serve. La presunzione che "il drone vola alto, quindi non identifica nessuno" non regge davanti al Garante. L'EDPB Linee Guida 3/2019 v2.0 al §9 lo dice esplicitamente: *"Le registrazioni ad alta quota rientrano nell'ambito di applicazione del RGPD solo se, in queste*

circostanze, i dati trattati possono essere correlati a una determinata persona." Il test è sull'identificabilità del materiale trattato e conservato, non sull'occhio nudo durante il volo. Una ripresa 4K a 80 m post-processata in 100% crop identifica targhe, abiti, taglio capelli — identificabile per combinazione di elementi (art. 4(1) GDPR).

Garante — 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: il "tanto le immagini termiche non mostrano volti" non funziona. Il Garante qualifica come dato personale anche le sagome contestualizzate, perché in combinazione con un intervento de visu della pattuglia possono ricondurre a persona identificata. Per il drone commerciale è il principio applicabile a qualunque payload (termico, RGB, multispettrale).

L'art. 35 par. 3 lett. c) GDPR impone DPIA per *"sorveglianza sistematica su larga scala di una zona accessibile al pubblico"* — formula che a prima vista non riguarda l'operatore UAS commerciale, ma che letta dall'EDPB GL 3/2019 §§ 7 e 136-138 copre molte configurazioni operative reali. La maggior parte degli operatori UAS italiani opera senza DPIA: per molti è legittimo (DPIA non scatta), per una minoranza significativa scatta e nessuno l'ha fatta. Questa guida distingue i due casi con riferimenti articolo-per-articolo.

Disclaimer: questa guida non sostituisce il parere di un DPO o di un legale privacy. La qualificazione di "rischio elevato" ex art. 35 GDPR dipende da fatti specifici della singola operazione (numero interessati, durata, modalità di trattamento, post-processing applicato). La sezione "Da verificare" finale elenca i punti che richiedono valutazione professionale per il caso concreto.

01 Quando il drone tratta dati personali

Il GDPR all'art. 4 par. 1 definisce "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente. Il punto cruciale per UAS è "indirettamente": l'identificabilità può derivare da combinazione di elementi (volto + abiti + luogo + orario + targa veicolo + edificio + ecc.).

Il trattamento (art. 4 par. 2) inizia alla raccolta, non al post-processing. Il raw file con volti riconoscibili è già un trattamento di dato personale, anche se cancellato 10 minuti dopo. Il blur eventuale è una misura di mitigazione documentata nella DPIA, non una scappatoia dal regolamento.

Configurazioni in cui il drone NON tratta dati personali

Scenario	Trattamento?	Perché
Ispezione tetto edificio industriale isolato, no persone in vista	No	Manca il "dato personale" — niente persone identificabili
Mappatura agricola di fondo proprio, no terzi nel raggio	No	Idem
Aerofotogrammetria a quote elevate (>120 m AGL) con GSD > 20 cm/pixel e nessun post-processing identificativo	No (probabile)	Test EDPB §9: nessuna correlazione possibile a persona determinata
Riprese filmiche nature/landscape senza presenza umana inquadrata	No	Idem

In questi casi, ROPA può non avere voce dedicata al drone, ma il ROPA aziendale resta dovuto se ci sono altri trattamenti (dipendenti, clienti).

Configurazioni in cui il drone tratta dati personali

Scenario	Trattamento?	Perché
Ripresa eventi sportivi con pubblico	Sì	Persone identificabili
Ispezione facciata condominio abitato con possibili volti a finestre/balconi	Sì	Trattamento incidentale
Sorveglianza periodica di cantiere/impianto con operai presenti	Sì	Persone identificabili + lavoratori → anche art. 4 L. 300/1970
Fotogrammetria area urbana, popolazione presente, GSD < 5 cm/pixel	Sì	Identificabilità in post-processing

Scenario	Trattamento?	Perché
Spraying agricolo con drone in confine di strada/abitato — telecamera attiva	Sì	Anche se finalità è agronomica

02 La deroga domestica: perché un operatore commerciale non la può invocare

L'art. 2 par. 2 lett. c) GDPR esclude dall'applicazione il trattamento "effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico". Sembra un'uscita facile per il pilota UAS "ricreativo" che pubblica video su YouTube. Non lo è.

L'EDPB Linee Guida 3/2019 §§ 12-14 chiarisce che la deroga è interpretata restrittivamente. Casi-chiave CGUE:

- C-101/01 Lindqvist (2003): la pubblicazione di dati personali su Internet esce dalla deroga anche se l'attività ha finalità personale
- C-212/13 Ryneš (2014): la videosorveglianza che inquadra anche parzialmente spazio pubblico (es. marciapiede davanti a casa) esce dalla deroga

Per un operatore UAS:

- Pilota che vola sul proprio giardino recintato, nessuno spazio pubblico inquadrato, nessuna pubblicazione → deroga applicabile
- Pilota "ricreativo" che pubblica video su YouTube/Instagram → fuori deroga, è titolare del trattamento a tutti gli effetti
- Operatore commerciale (P.IVA, fattura al cliente) → mai deroga domestica, sempre dentro GDPR

03 La base giuridica: art. 6 e perché il "consenso" quasi mai funziona

L'art. 6 par. 1 GDPR elenca le 6 basi giuridiche del trattamento:

a) Consenso dell'interessato b) Contratto con l'interessato c) Obbligo legale del titolare d) Tutela interessi vitali dell'interessato o di terzi e) Compito di interesse pubblico o pubblici poteri f) Legittimo interesse del titolare o di terzi

Per le operazioni UAS commerciali:

- (a) Consenso: impraticabile in spazio pubblico. Non si raccoglie il consenso di 200 passanti prima di volare.
- (b) Contratto: applicabile solo verso il cliente committente (non verso terzi ripresi incidentalmente).
- (c) Obbligo legale: raro per UAS privato; può scattare per PA che gestisce sicurezza pubblica via drone.
- (d) Vitali: emergenze, rarissimo.
- (e) Interesse pubblico: solo per soggetti pubblici (PA, ENPS, ecc.).
- (f) Legittimo interesse: la base giuridica più comune per UAS commerciale, ma richiede test di bilanciamento (EDPB GL 3/2019 §§ 30-40) documentato per iscritto.

Il test di bilanciamento valuta tre elementi: (1) esistenza dell'interesse legittimo del titolare; (2) necessità del trattamento per perseguirlo; (3) prevalenza dell'interesse del titolare rispetto ai diritti dell'interessato, tenute conto le sue "ragionevoli aspettative".

L'EDPB GL 3/2019 §40 chiarisce un punto cruciale:

"La presenza di segnaletica che informa l'interessato in merito alla videosorveglianza è del tutto irrilevante al fine di determinare ciò che un interessato può oggettivamente aspettarsi."

Il cartello "Attenzione, volo drone in corso" non è sufficiente a giustificare il bilanciamento. È solo informativa (art. 13) e non sostituisce il test di necessità.

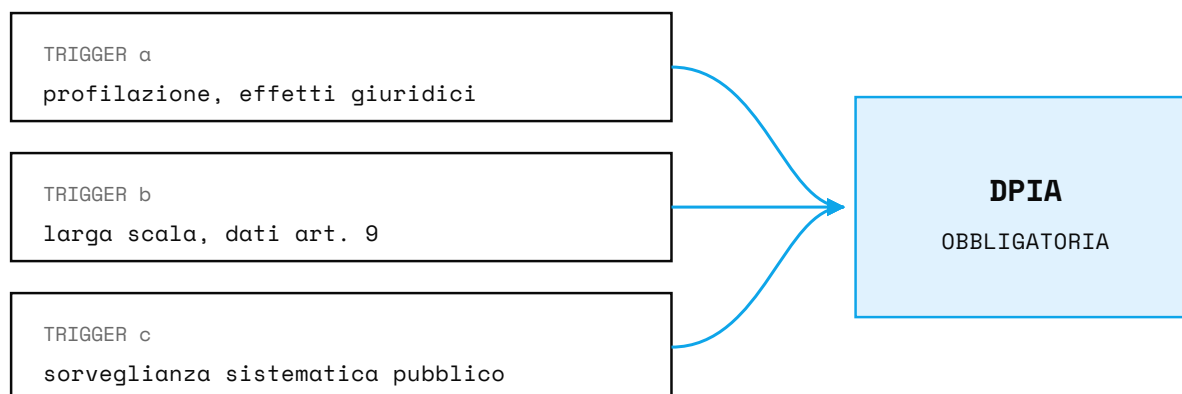
04 Quando scatta la DPIA obbligatoria: tre trigger

L'art. 35 par. 1 GDPR è la cornice generale:

"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali."

L'art. 35 par. 3 elenca tre casi di DPIA obbligatoria di diritto:

- (a) Valutazione sistematica e globale di aspetti personali con effetti giuridici (es. profilazione automatica)
- (b) Trattamento su larga scala di categorie particolari (art. 9) o dati relativi a condanne penali
- (c) Sorveglianza sistematica su larga scala di una zona accessibile al pubblico



SCHEMA – I TRE TRIGGER DELL'ART. 35 §3 GDPR: NE BASTA UNO

A questi si aggiungono i casi del Provvedimento del Garante n. 467 dell'11 ottobre 2018 ([doc web 9058979](#)) che elenca 12 tipologie di trattamenti soggetti a DPIA obbligatoria in Italia, e i criteri WP248 dell'Article 29 Working Party (recepiti dall'EDPB) — la regola dei "2 criteri su 9".

La regola dei 2 criteri WP248

Se l'operazione attiva almeno 2 dei 9 criteri sotto, la DPIA è da considerare obbligatoria:

1. Valutazione/scoring
2. Decisioni automatizzate con effetti legali o significativi
3. Monitoraggio sistematico
4. Categorie particolari o dati di natura particolarmente personale
5. Larga scala
6. Combinazione/incrocio di dataset
7. Interessati vulnerabili (minori, lavoratori, pazienti)
8. Nuove tecnologie
9. Quando il trattamento di per sé "impedisce all'interessato di esercitare un diritto o utilizzare un servizio"

Per UAS la combinazione tipica è: 3 (monitoraggio) + 5 (larga scala) + 8 (nuove tecnologie) → DPIA obbligatoria.

"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: la DPIA è una condizione di legittimità ex ante, non un documento "da produrre se arriva l'ispezione". Farla dopo l'inizio del trattamento è violazione autonoma — sanzionata €100.000 nel caso Realmaps insieme al complesso degli altri inadempimenti.

L'EDPB GL 3/2019 §136 chiude:

"Date le finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione biometrica di soggetti sospetti), è ragionevole supporre che molti casi di videosorveglianza richiederanno una valutazione d'impatto sulla protezione dei dati."

Il drone con payload video rientra pienamente nella "videosorveglianza" come definita dall'EDPB.

05 Come si fa una DPIA per operazione UAS

L'art. 35 par. 7 GDPR definisce il contenuto minimo della DPIA:

- a) Descrizione sistematica del trattamento e delle finalità b) Valutazione di necessità e proporzionalità
- c) Valutazione dei rischi per diritti e libertà degli interessati d) Misure previste per affrontare i rischi (mitigazioni)

Workflow operativo (7 step)

1. Mappare l'operazione: tipo missione, durata, area, persone potenzialmente coinvolte
2. Pre-valutazione (threshold assessment): applicare i 9 criteri WP248. Se $\geq 2 \rightarrow$ procedere a DPIA. Documentare comunque la decisione anche se "no DPIA", per accountability art. 5 par. 2
3. Descrizione sistematica (art. 35(7)(a)): cosa viene trattato, da chi, dove, perché, con quali strumenti, conservazione
4. Test di necessità e proporzionalità (art. 35(7)(b)): la finalità si raggiunge con meno dati? Risoluzione minima utile? Blur in tempo reale possibile?
5. Valutazione dei rischi (art. 35(7)(c)): per ogni rischio identificato (riconoscimento identificativo, comunicazione non autorizzata, perdita dati, ecc.), valutare gravità $\times$ probabilità

6. Misure di mitigazione (art. 35(7)(d)): tecniche (blur, crittografia, cancellazione automatica) + organizzative (DPA con fornitori, nomina art. 29 del pilota, formazione)
 7. Consultazione preventiva art. 36 GDPR se la DPIA rivela rischio residuo elevato nonostante misure → istanza al Garante prima del trattamento
-

06 **ROPA, informativa, DPO: gli altri 3 obblighi che vengono prima della DPIA**

Spesso si parla di DPIA come fosse l'unico adempimento privacy del drone. Non è. Tre obblighi vengono prima e si applicano molto più ampiamente.

Registro delle attività di trattamento (ROPA) — art. 30

Obbligatorio per tutti i titolari, con esonero limitato per imprese < 250 dipendenti che effettuano trattamenti occasionali, non comprensivi di categorie particolari e che non possano arrecare rischio.

Per un'azienda UAS commerciale, l'esonero quasi mai si applica: il trattamento per riprese aeree è ricorrente, non occasionale. ROPA obbligatorio.

Contenuto minimo per la voce "Riprese aeree UAS":

- Finalità del trattamento (es. ispezione strutturale per cliente X)
- Categorie di interessati (passanti, dipendenti del cliente, ecc.)
- Categorie di dati (immagini, video, metadata di volo)
- Destinatari (cliente, eventuale cloud storage, eventuali autorità)
- Trasferimenti extra-UE (se cloud è fuori UE)
- Termini di conservazione
- Misure di sicurezza tecniche e organizzative

Informativa (artt. 13-14)

L'art. 13 disciplina l'informativa all'interessato. Per la videosorveglianza/drone l'EDPB GL 3/2019 §§ 109-122 propone un modello a due livelli:

- Primo livello: cartello area di volo con titolare + finalità + base giuridica + QR a informativa estesa
- Secondo livello: pagina web accessibile con tutti i contenuti EDPB §7 (DPO, conservazione, diritti, autorità di controllo)

Il caso Mark Bologna ([doc web 10070348](#)) ha sanzionato €5.000 per informativa assente, oltre che per autorizzazione ITL preventiva mancante (10 telecamere in bar).

DPO (Responsabile della protezione dei dati) — art. 37

Obbligatorio se l'attività core è:

- Monitoraggio regolare e sistematico su larga scala (art. 37 par. 1 lett. b), o
- Trattamento di categorie particolari su larga scala (art. 37 par. 1 lett. c)

Per la ditta UAS media: di norma DPO non obbligatorio, ma DPO esterno raccomandato se >1 cantiere ricorrente di sorveglianza/monitoraggio.

07 Configurazioni tipiche dell'operatore UAS — DPIA sì/no per 6 scenari

#	Scenario	DPIA obbligatoria?	Perché
A	Ispezione tetto edificio industriale isolato, no persone	No	Manca il "dato personale"
B	Ispezione facciata condominio abitato, possibili volti a finestra	Sì, raccomandata	Trattamento incidentale; rischio elevato per "ragionevoli aspettative" interessati (EDPB §§ 36-38). DPIA documenta misure di minimizzazione
C	Ripresa evento pubblico con pubblico identificabile da drone	Sì	Sorveglianza sistematica su larga scala (art. 35(3)(c)). Se c'è riconoscimento facciale: art. 9 (biometrici) → DPIA + base giuridica rafforzata
D	Sorveglianza periodica/quotidiana area di cantiere o impianto, con operai	Sì	Doppia base: art. 35(3)(c) + art. 114 Codice Privacy (lavoratori) → autorizzazione preventiva ITL o accordo sindacale obbligatorio
E	Fotogrammetria area urbana per topografia, popolazione presente	Caso per caso — propendere per Sì	Test EDPB § 9: se risoluzione + post-processing consentono identificazione → DPIA

#	Scenario	DPIA obbligatoria?	Perché
F	Spraying agricolo su fondi propri, no persone nel raggio	No	No dato personale. Attenzione se confine con strada/abitazioni: valutare misure di minimizzazione (no camera attiva durante spray, o telecamera angolata)

Trigger combinati che spostano sempre verso "DPIA sì" (regola "2 criteri su 9"):

1. Monitoraggio sistematico (≥ 1 criterio)
2. Uso di "nuove tecnologie" — il drone con AI di riconoscimento entra qui
3. Trattamento su larga scala (numero interessati indefinito in spazio pubblico)
4. Categorie particolari (es. ripresa folla a manifestazione → opinioni politiche, art. 9)
5. Interessati vulnerabili (minori in parchi, pazienti in strutture sanitarie)

Se ≥ 2 di questi criteri → DPIA da fare prima del volo.

08 Le 5 trappole comuni

Trappola 1 — "Volo a 80 m, non si riconosce nessuno"

Falso. EDPB §9 (citazione integrale all'inizio dell'articolo): il test è sull'identificabilità nel materiale trattato e conservato, non sull'occhio nudo durante il volo. Una ripresa 4K a 80 m post-processata in 100% crop identifica targhe, abiti, taglio capelli → identificabile per combinazione di elementi (art. 4(1) GDPR).

Trappola 2 — "Posso blurrare i volti dopo, quindi GDPR non si applica al raw"

Falso. Il trattamento inizia alla raccolta (art. 4(2)). Il raw file con volti riconoscibili è già un trattamento di dato personale, anche se cancellato 10 minuti dopo. Il blur è una misura di mitigazione, non una scappatoia. Va documentato come misura tecnica nella DPIA (art. 35(7)(d)).

Trappola 3 — "Il committente è titolare, io sono solo il pilota"

Dipende, ma di solito falso. L'operatore UAS che decide come volare (rotta, telecamera, conservazione raw) è co-titolare o responsabile, non meramente esecutore. Se il committente fornisce solo il "cosa" (es. "fai vedere i tetti"), l'operatore UAS resta titolare per le scelte tecniche-privacy. La nomina a responsabile art. 28 GDPR va fatta per iscritto con clausole specifiche, altrimenti

il pilota risponde autonomamente. Caso Garante Treviso 2024: il Comune è stato sanzionato anche per mancanza di nomina art. 28 verso il fornitore tecnologico.

Trappola 4 — "Sono ricreativo, mi salva la deroga domestica"

Quasi sempre falso se posti su social. EDPB §§ 12-14: la deroga "personale o domestica" (art. 2(2)(c) GDPR) è interpretata restrittivamente. La pubblicazione su Internet di video drone esce dalla deroga (CGUE C-101/01 Lindqvist). Inoltre, se il volo si estende anche solo parzialmente a spazio pubblico → fuori deroga (CGUE C-212/13 Ryneš).

Trappola 5 — "DPIA l'ho fatta nel 2020, è pronta per sempre"

Falso. Art. 35 par. 11 GDPR: *"il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio"*. L'EDPB §20 raccomanda riesame annuale. Cambia il drone, il sensore, la zona di operazione, la finalità del cliente → DPIA da rivedere.

09 Sanzioni e casi Garante 2020-2026 verificati

Quadro sanzionatorio GDPR

- Art. 83 par. 4 GDPR — sanzioni "fascia bassa": fino a €10 milioni o 2% fatturato annuo mondiale (il maggiore). Per: DPIA omessa, DPO non designato, ROPA mancante, privacy by design assente
- Art. 83 par. 5 GDPR — sanzioni "fascia alta": fino a €20 milioni o 4% fatturato annuo mondiale. Per: violazioni principi (art. 5), basi giuridiche (art. 6), categorie particolari (art. 9), diritti interessati, trasferimenti extra-UE
- Codice Privacy art. 166 — il Garante applica le sanzioni GDPR + sanzioni penali specifiche (art. 167 — fino a 6 anni di reclusione per trattamento illecito + diffusione)

Casi verificati con doc web

Data	Soggetto	Doc web	Fatti	Sanzione
3/9/2021	Comune Bari, Roma	9696781	Istruttorie su uso droni Covid (assembramenti, illeciti ambientali, misurazione febbre)	Istruttorio

Data	Soggetto	Doc web	Fatti	Sanzione
	Capitale, ASL Roma 3		Ostia) — richiesta DPIA, base giuridica, retention	
16/11/2023	Comune Castel Goffredo (MN)	9963486	Telecamera audio-video presso Comando Polizia Locale senza autorizzazione art. 4 L. 300/70; comunicazione illecita	€50.000
4/7/2024	Comune di Treviso	10050298	Droni con telecamere termiche + app "TrevisoSicura" — segnalazioni reati senza DPA fornitore, ruoli art. 28 errati	€7.000 (per app; uso droni archiviato per dichiarazione di non identificazione)
17/7/2024	Mark s.r.l.s. (Bologna)	10070348	10 telecamere in bar senza cartellonistica, no autorizzazione ITL preventiva	€5.000
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
4/6/2025	Comune di Recco (GE)	10163530	Videosorveglianza fissa OCR su conferimento rifiuti — analoga per principi al drone	€5.000

Pattern degli errori (ricorrono in 8/10 casi):

- Informativa assente o inadeguata (art. 13)
- Base giuridica non specificata o errata (art. 6)
- DPIA omessa (art. 35)
- ROPA assente o incompleto (art. 30)
- Nomina art. 28 omessa
- Privacy by design ignorato (art. 25)

Punto editoriale critico: i casi UAS sanzionati documentati riguardano enti pubblici (Polizia Locale, Comuni). Non sono emersi nella ricerca casi di operatori UAS privati commerciali già sanzionati per DPIA omessa — il quadro normativo è identico per il privato, ma il rischio è asimmetrico perché il Garante ha iniziato dalle PA visibili. La logica vorrebbe che i privati siano i prossimi.

10 Checklist privacy pre-flight: 12 punti

Pensata come complemento alla checklist di volo. Si compila in fase di pianificazione missione, prima di prenotare il volo.

- ☐ 1. Mappare il volo: c'è ragionevole probabilità di riprendere persone identificabili (anche da elementi non-volto: abiti, targa, edificio)? Se sì → procedi sotto
- ☐ 2. Verificare la deroga domestica: scopo strettamente personale + no pubblicazione + no spazio pubblico → fuori GDPR. Altrimenti → dentro GDPR
- ☐ 3. Identificare titolare e ruoli: chi è titolare? Cliente committente generico (tu titolare) o committente che ha definito mezzi e finalità (tu responsabile art. 28)?
- ☐ 4. Verificare ROPA aziendale art. 30: il trattamento "ripresa aerea per cliente X" è una voce nel ROPA?
- ☐ 5. Definire la base giuridica art. 6: tipicamente 6(1)(b) contratto o 6(1)(f) legittimo interesse. Consenso impraticabile in spazio pubblico
- ☐ 6. Eseguire la pre-valutazione (threshold assessment): criteri WP248 ≥ 2 su 9? Se sì → DPIA. Documentare la decisione anche se NO
- ☐ 7. Se DPIA obbligatoria, scrivere art. 35(7): (a) descrizione trattamenti, (b) necessità/proporzionalità, (c) rischi per interessati, (d) misure mitigazione
- ☐ 8. Verificare necessità DPO art. 37: di norma no per ditta UAS media, ma DPO esterno raccomandato se sorveglianza ricorrente
- ☐ 9. Preparare informativa art. 13: cartello area di volo + sito web + (se evento) consegna a hostess
- ☐ 10. Misure tecniche by design (art. 25): blur automatico, crittografia storage, rotazione chiavi, cancellazione automatica del raw dopo X giorni
- ☐ 11. Verifica art. 114 Codice Privacy: se nei ripresi ci sono lavoratori → accordo sindacale o autorizzazione ITL prima del volo
- ☐ 12. Consultazione preventiva art. 36 GDPR: se la DPIA rivela rischio residuo elevato → istanza al Garante prima del trattamento

11 Come Hovra rende sostenibile la compliance privacy di una missione UAS

Hovra Own integra nel flusso missione i template e i workflow privacy che oggi sono spesso compilati a mano (o non compilati affatto):

- Threshold assessment pre-missione: per ogni pianificazione di volo, lo strumento applica i 9 criteri WP248 e segnala se serve DPIA
- Template DPIA per UAS: documento art. 35(7) pre-compilato con descrizione tipica (rotta, telecamera, conservazione) — da personalizzare con i dati del caso concreto
- ROPA aziendale UAS: voce "Riprese aeree UAS" pre-strutturata con tutte le colonne art. 30 + integrazione automatica delle missioni svolte
- Informativa a due livelli: generatore di cartello area di volo (primo livello) + pagina web di secondo livello editabile
- DPA art. 28: modello di contratto tra operatore UAS e fornitori (cloud storage immagini, software flight log)
- Retention policy: cancellazione automatica raw dopo finestra configurabile, log della cancellazione per accountability

→ [Scopri il modulo Privacy Compliance su hovra.it](#) → Articoli correlati: [CB#003 Patentino A2/STS](#) · [CB#005 Impresa agricola o servizi](#) · [CB#006 U-Space Italia 2026](#) · [CB#014 Sanzioni Garante 2020-2026](#)

12 Bibliografia

Fonti primarie

- Regolamento (UE) 2016/679 (GDPR) del Parlamento europeo e del Consiglio del 27 aprile 2016. [EUR-Lex](#). Artt. 4(1), 4(2), 5, 6, 9, 13-14, 25, 28, 30, 35, 36, 37, 82, 83
- D.Lgs. 30 giugno 2003 n. 196 (Codice Privacy) modificato da D.Lgs. 10 agosto 2018 n. 101. [Normattiva](#). Artt. 2-ter (base giuridica PA), 114 (controllo a distanza lavoratori), 166-167 (sanzioni)
- Provvedimento Garante n. 467 dell'11 ottobre 2018 — Elenco trattamenti soggetti a DPIA obbligatoria. [doc web 9058979](#)
- WP29 — Linee guida DPIA WP 248 rev. 01 (recepita EDPB). Criteri "rischio elevato" (9 criteri), regola 2 su 9
- L. 20 maggio 1970 n. 300 (Statuto dei Lavoratori) art. 4 — controlli a distanza
- Regolamento (UE) 2019/947 — operazioni UAS, art. 14 (registrazione operatore)

Linee guida interpretative

- EDPB — Linee Guida 3/2019 v2.0 sul trattamento di dati personali attraverso dispositivi video. Adottate 29/1/2020. [EDPB](#). §§ 7-9 (sorveglianza sistematica, alta quota), §§ 11-14 (deroga

domestica), §§ 30-40 (legittimo interesse, ragionevoli aspettative), §§ 109-122 (informativa due livelli), §§ 136-138 (DPIA)

Giurisprudenza CGUE rilevante

- CGUE C-101/01 Lindqvist (6 novembre 2003) — pubblicazione su Internet esce dalla deroga domestica
- CGUE C-212/13 Ryneš (11 dicembre 2014) — videosorveglianza che inquadra spazio pubblico esce dalla deroga domestica

Provvedimenti Garante citati

- [doc web 10050298 — Treviso 4/7/2024](#) — droni telecamere termiche + app TrevisoSicura
- [doc web 10163530 — Recco 4/6/2025](#) — videosorveglianza OCR
- [doc web 10070348 — Mark Bologna 17/7/2024](#) — 10 telecamere bar
- [doc web 9963486 — Castel Goffredo 16/11/2023](#) — telecamera audio-video Polizia Locale
- [doc web 9696781 — istruttorie Covid 3/9/2021](#) — Bari + Roma Capitale + ASL Roma 3
- [doc web 10110241 — Realmaps 16/1/2025](#) — liste immobili
- [doc web 10128005 — ARSAC 13/3/2025](#) — geolocalizzazione GPS smartworking

Articoli correlati nella serie

- [CB#003 — Patentino A2 e STS](#) — DPIA si aggiunge ai requisiti ENAC
- [CB#005 — Impresa agricola o servizi UAS?](#) — natura giuridica cambia esonero ROPA art. 30
- [CB#006 — U-Space Italia 2026](#) — dati Network ID (posizione operatore) sono dati personali del pilota
- [CB#014 — Sanzioni Garante 2020-2026](#) — case study completo dei 10 provvedimenti rilevanti

Questo documento ha finalità informative e divulgative. Non sostituisce in alcun caso il parere di un Data Protection Officer o di un legale specializzato in privacy. La qualificazione di "rischio elevato" ex art. 35 GDPR e l'applicabilità dei criteri WP248 dipendono dal caso concreto.

Nimber S.r.l.