

DPIA DEL SISTEMA WHISTLEBLOWING

Revisione 2.0 del 22/09/2026 - approvazione AU: ____/____/____

DPIA del sistema whistleblowing

Società	C.N. Costruzioni Generali S.p.A.
Codice documento	WB-13
Versione	Revisione 2.0 del 22/09/2026
Stato	Valutazione da completare dal Titolare con dati del servizio e parere DPO; nessun esito già approvato
Predisposto il	22/09/2026
Entrata in vigore	Dalla data effettiva indicata nella nuova determinazione AU, senza retrodatazione
Approvazione	Amministratore Unico - firma e data in calce

DATI DA COMPLETARE PRIMA DELLA FIRMA

Sede legale: Via Giovanni Amendola 172/E - 172/C, 70126 Bari. DPO: Roberto Froio, info@robertofroio.net. Restano da documentare provider, hosting, subresponsabili e il gestore esterno indipendente per doppio conflitto. Le relative evidenze sono necessarie prima della dichiarazione di completa operatività.

1. Descrizione del trattamento

Il trattamento comprende ricezione tramite piattaforma web, canale orale e incontro; registrazione del fascicolo; interlocuzione; valutazione; istruttoria; azioni correttive; report aggregati; conservazione e cancellazione. Può riguardare dati particolari, giudiziari e informazioni ad alto rischio reputazionale e lavoristico.

2. Necessità e proporzionalità

Requisito	Misura
Finalità determinate	Solo gestione di violazioni apprese nel contesto lavorativo e protezione delle persone segnalanti.
Minimizzazione	Separazione identità/contenuto, dati manifestamente inutili cancellati, accesso per fascicolo.
Trasparenza	Informativa WB-04, informazioni sui canali e sui diritti con limitazioni previste dalla legge.
Conservazione	WB-07: massimo cinque anni dall'esito finale, con termini più brevi per copie e audio.
Diritti	Gestione con DPO e limitazioni motivate per tutelare la riservatezza.
Responsabili	Contratti art. 28, subfornitori dichiarati, localizzazione e misure verificate.

3. Analisi dei rischi

Rischio	Inerente	Misure	Residuo obiettivo, da verificare
Identificazione del segnalante	Molto alto	Segregazione, cifratura, accesso nominativo, report anonimi	Medio
Accesso abusivo interno	Alto	MFA, least privilege, log, profili separati, test	Basso/medio

Rischio	Inerente	Misure	Residuo obiettivo, da verificare
Invio errato o copia locale	Alto	Divieto e-mail ordinaria, watermark/codice, formazione, cancellazione copie	Medio
Ritorsione	Molto alto	Riservatezza, canale conflitti, monitoraggio e protocollo urgente	Medio
Alterazione o distruzione prove	Alto	Logging, backup, integrità, conservazione controllata	Basso/medio
Dati eccedenti o falsi	Alto	Minimizzazione, verifica pertinenza, contraddittorio e cancellazione	Medio
Fornitore compromesso	Alto	Art. 28, audit, cifratura, subfornitori, incident response	Medio
Conflitto Gestore	Alto	Sostituto, routing e soggetto esterno per doppio conflitto	Basso/medio
Mancata cancellazione	Medio/alto	Scadenziario, verbale cancellazione, test backup	Basso

4. Misure da completare prima del go-live

- nominare e formare il Sostituto;
- confermare sede dei dati, provider e subfornitori;
- concludere accordo art. 28 GDPR;
- attivare MFA e log non modificabili;
- testare routing conflitto e cancellazione dai backup;
- completare recapito DPO e informativa sul sito;
- documentare la consultazione ex art. 4 e le osservazioni, prima della revisione sostanziale del canale;
- definire soggetto esterno per doppio conflitto.

5. Valutazione conclusiva

ESITO DEL TITOLARE, ACQUISITO IL PARERE DEL DPO

☐ Rischio residuo accettabile con misure completate ☐ Ulteriori misure necessarie ☐ Consultazione preventiva dell'Autorità da valutare

Titolare / Amministratore Unico	Dott. Silvestro Carbotti Data effettiva: ____/____/____ Firma: _____
DPO	Dott. Roberto Froio Data effettiva: ____/____/____ Firma: _____
Gestore	Melissa Cuccovillo Data effettiva: ____/____/____ Firma: _____
Responsabile IT	Ing. Francesco Fiorella - funzione IT Data effettiva: ____/____/____ Firma: _____

6. Dati ed evidenze per completare la valutazione

Il Titolare identifica provider, contratto, ubicazione di server e backup, subresponsabili, amministratori tecnici, trasferimenti e relative garanzie; documenta flussi di dati e separazione identità/contenuto. IT produce prove su cifratura, chiavi, autenticazione, profili, log, backup, ripristino, cancellazione e percorsi di conflitto. Il Gestore verifica oralità, incontro e interlocuzione.

Per ogni rischio si registrano probabilità e impatto, misura, responsabile, evidenza e rischio residuo effettivo. I valori in tabella sono obiettivi e non dimostrano l'implementazione delle misure. Il DPO rende un parere

indipendente e sorveglia il processo; il Titolare decide e documenta anche l'eventuale scostamento dal parere. Se permane un rischio elevato in assenza di misure idonee, si applica la consultazione preventiva ex art. 36 GDPR prima del trattamento interessato.