INFORMATIVA WHISTLEBLOWING

SEGNALAZIONI WHISTLEBLOWING

A seguito dell'entrata in vigore del D. Lgs 24/2023 in materia di Whistleblowing, DAOS Group ha predisposto i canali per la segnalazione di eventuali illeciti e irregolarità aziendali.
DAOS Group mira a mantenere un ambiente in cui le comunicazioni aperte e oneste siano la regola e non l'eccezione, con il desiderio che tutti i dipendenti e i collaboratori si sentano a proprio agio nel porre domande o esprimere dubbi quando ritengono che si siano verificate delle possibili violazioni.
Con l'espressione Whistleblowing si fa riferimento alla segnalazione come manifestazione di senso civico, che contribuisce a far emergere e a prevenire situazioni che pregiudichino la buona amministrazione o l'interesse pubblico.
Chiunque sia a conoscenza di irregolarità che potrebbero comportare violazioni e/o illeciti può effettuare una segnalazione Whistleblowing.
DAOS Group garantisce la riservatezza e l'anonimato di chi vorrà fare una segnalazione e delle informazioni fornite nel rispetto della legge.

CANALI DI SEGNALAZIONE

I canali per poter effettuare una segnalazione sono i seguenti:

- attraverso il portale Signalethic al link https://fusel.signalethic.it/signalethic/home
- contattando telefonicamente il Gestore delle Segnalazioni ai recapiti sotto indicati;
- nell'apposita sezione del sito ANAC https://whistleblowing.anticorruzione.it/#/

Si ricorda che i canali per le segnalazioni Whistleblowing non sono appropriati per gestire questioni personali o relative al contratto di lavoro, rapporti con il supervisore o altri colleghi non rientranti nelle violazioni del Codice Etico o del D. Lgs 24/2023.
Il Gestore delle Segnalazioni Whistleblowing, per DAOS Group, è:

DOCUVERSE - C.F./P.IVA 04385230240, con sede legale in Vicenza (36100), Via dell'Edilizia 11
PEC: docuverse@pec.it
+39 0444 419325

CONSIGLI PER L'ANONIMATO

Signalethic è stato progettato seguendo i principi della privacy e sicurezza by design e by default, ovvero integrando i requisiti del GDPR nello sviluppo del software e per impostazione predefinita, sin dalla progettazione. Il traffico verso il portale Signalethic è cifrato in transit (in transito) mentre i dati conservati nella piattaforma sono cifrati at rest (a riposo o a database).
Per proteggere le segnalazioni:
• utilizzare dispositivi privati e di cui si ha il controllo per effettuare le segnalazioni o per consultare le segnalazioni già effettuate;
• utilizzare se possibile una finestra di navigazione in incognito;
• conservare le credenziali in luoghi protetti e dove non ci sia il rischio di condividerle con nessuno;
• assicurarsi di non effettuare segnalazioni o non accedere al portale Signalethic in pubblico o in luoghi dove l'attività effettuata sullo schermo possa essere vista da altri;
• accedere al portale Signalethic solo tramite una connessione internet sicura e un network privato così da proteggere il traffico internet prima che arrivi alla piattaforma.