Deloitte.
Legal

Compliance Today
Aggiornamento Whistleblowing

Keep updated for a safe business

MAKING AN IMPACT THAT MATTERS since 1845

Deloitte Legal, December 2021

Le ultime FAQ dell’ANAC

L’ ANAC, l’Autorità Nazionale Anti Corruzione, ha pubblicato in data 17 dicembre 2021 le FAQ aggiornate in materia di Anticorruzione - whistleblowing relative alla Delibera n. 469 del 9 giugno 2021.

1. Procedura di gestione, rivelazione dell'identità e conservazione delle segnalazioni

La procedura di gestione delle segnalazioni whistleblowing rientra tra le **misure generali di prevenzione della corruzione da introdurre nel PTPCT**.

Il PTPCT può anche rinviare, per maggiori dettagli, ad un apposito atto organizzativo adottato dall'Organo di indirizzo.

Il segnalante, ove lo ritenga, può svelare la propria identità al RPCT.

I dati raccolti vanno conservati per **un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati** (e.g., per le segnalazioni ricevute da ANAC, è stato previsto un termine minimo di conservazione pari almeno a 10 anni).

Il **termine** di conservazione delle segnalazioni **deve essere fissato per tutte le segnalazioni**, qualsiasi sia il canale utilizzato dal segnalante.

2. Il «custode» dell'identità del segnalante

L'istituzione della figura	L'istituzione della figura del «custode» **non è obbligatoria**. La figura del custode funge da **ulteriore garanzia** per la tutela della riservatezza del segnalante.
Profili professionali	Il «custode» deve possedere i requisiti di **terzietà e imparzialità**. Il «custode» può **coincidere con il RPCT**.
Trattamento dei dati personali	Il «custode» deve essere **autorizzato al trattamento dei dati personali** ai sensi dell'art. 4, par. 10, 29, 32 del Regolamento UE 2016/679.
«Sblocco" dell'identità del segnalante	Il RPCT può avere accesso all'identità del segnalante solo dietro **espresso consenso del «custode» dell'identità**. I **casi** e le **motivazioni** in presenza delle quali il custode è autorizzato a disvelare l'identità del segnalante al RPCT devono essere disciplinate nel PTPCT, o nell'atto organizzativo cui rinvia il Piano con cui si definisce la procedura. Se il custode coincide con il RPCT, il RPCT è l'unico soggetto competente a sbloccare i dati identificativi del segnalante. In tale ipotesi il sistema deve registrare l'accesso all'identità da parte del RPCT.

3. Gruppo di lavoro a supporto del RPCT

Accesso alle informazioni

- I soggetti del gruppo che possono avere accesso alle informazioni e ai dati contenuti nella segnalazione devono essere preventivamente individuati dall'amministrazione o dall'ente nel PTPCT o nell'atto organizzativo cui il Piano rinvia.
- Oltre al RPCT, il coordinatore del gruppo può richiedere al custode di accedere all'identità del segnalante

Responsabilità dei componenti

- È opportuno che le amministrazioni introducano nei codici di comportamento forme di responsabilità specifica in capo sia al RPCT che riceve e gestisce le segnalazioni di whistleblowing, sia a tutti gli altri soggetti - ivi inclusi i componenti del gruppo di lavoro - che nell'amministrazione possano venire a conoscenza delle segnalazioni.

Accesso alla piattaforma

- Ciascun componente del gruppo di lavoro può accedere alla Piattaforma informatica di gestione delle segnalazioni separatamente dal RPCT per svolgere le necessarie attività in merito alle segnalazioni assegnategli.

Assegnazione della segnalazione

- L'assegnazione di una segnalazione whistleblowing deve essere, di volta in volta, disposta dal RPCT.
- Il soggetto cui è stata assegnata la segnalazione non può riassegnarla a sua volta ad un collega/ufficio.
- L'assegnazione di una segnalazione whistleblowing può essere revocata dal RPCT con apposita motivazione.

4. La piattaforma di gestione delle segnalazioni

Chiarezza e trasparenza

L'Amministrazione o l'ente deve rendere pubblico il sistema informatico di gestione delle segnalazioni whistleblowing nella home page del proprio sito istituzionale in modo chiaro e visibile.

Pubblicazione indirizzo web

L'indirizzo web della piattaforma deve essere raggiungibile da Internet, ma l'amministrazione/ente può decidere di non renderlo pubblico sul sito istituzionale.

Dispositivi firewall e proxy

Nel caso in cui l'accesso alla piattaforma informatica sia mediato da dispositivi firewall o proxy, l'Amministrazione deve garantire la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione anche mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione.

Registrazione degli accessi

La piattaforma deve registrare gli accessi alla piattaforma da parte dei diversi utenti, nel rispetto nelle previsioni in materia di sicurezza informativa e di protezione dei dati personali.

Il disegno di legge di delegazione europea 2021

Il recepimento della Direttiva UE 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

5. Protezione delle persone che segnalano violazioni del diritto dell'Unione (imprese pubbliche e private)

Entro il **17 dicembre 2021**, l'Italia avrebbe dovuto recepire la Direttiva 2019/1937 emanata dal Parlamento Europeo, che prevede per le organizzazioni che impieghino **almeno 50 lavoratori** l'obbligo di istituire canali di segnalazione interni per la denuncia di violazioni del diritto dell'UE.

Il termine è esteso al **17 dicembre 2023** in caso di imprese con **più di 50 e meno di 250 lavoratori**.

In data 16 dicembre 2021, la Camera dei Deputati ha approvato, in prima lettura, il disegno di legge "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione Europea - Legge di delegazione europea 2021".

Il disegno di legge si compone di 20 articoli e un allegato A e contiene le deleghe per il recepimento di 10 direttive europee.

Tra le direttive europee inserite nell'Allegato A vi è la **direttiva UE 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.**

Disegno di legge di delegazione europea 2021

I **settori di business** e gli ambiti di attività che saranno interessati dalla Direttiva sono, a mero titolo esemplificativo, i seguenti:

- Appalti pubblici
- Servizi, prodotti e **mercati finanziari** e prevenzione del riciclaggio
- Sicurezza e **conformità dei prodotti**
- Sicurezza dei **trasporti**
- Tutela dell'**ambiente**
- Radioprotezione e sicurezza **nucleare**
- **Sicurezza degli alimenti** e dei mangimi e salute e benessere degli animali
- **Salute pubblica**
- **Protezione dei consumatori**
- Tutela della vita privata e **protezione dei dati personali** e sicurezza delle reti e dei sistemi informativi
- Violazioni che ledono gli **interessi finanziari dell'Unione**

Contact us:

Josephine Romano
Head of Corporate Compliance
Email: joromano@deloitte.it

Francesco Paolo Bello
Head of Public and Admin Law
Email: fbello@deloitte.it

Paola Gribaldo
Email: pgribaldo@deloitte.it

Cecilia Pontiggia
Email: cpontiggia@deloitte.it

Marianna Regillo
Email: mregillo@deloitte.it

Mattia Geraci
Email: mgeraci@deloitte.it

Deloitte.
Legal