FAQ in materia di Anticorruzione - whistleblowing

La sezione è stata aggiornata il 17 dicembre 2021

1.1. Come va disciplinata la procedura di gestione delle segnalazioni di whistleblowing?
La tutela del whistleblower rientra a pieno titolo tra le misure generali di prevenzione della corruzione da introdurre nel PTPCT di ogni amministrazione. Il PTPCT può anche rinviare, per maggiori dettagli, ad uno apposito atto organizzativo adottato dall'Organo di indirizzo. In ogni caso, l'Amministrazione è tenuta a disciplinare, in conformità alle presenti Linee guida, le modalità, preferibilmente informatiche, per la ricezione e la gestione delle segnalazioni di *whistleblowing*, definendo, e tra l'altro, i tempi e i soggetti responsabili

Parole chiave: tutela whistleblower -misura di prevenzione della corruzione-PTPCT-atto organizzativo- gestione segnalazioni -modalità informatiche- definizione dei tempi- individuazione soggetti responsabili
Fonti normativa: Delibera 469 del 9.06.2021 recante linee guida in materia di whistleblowing

1.2. La funzione del custode dell'identità è obbligatoria per le piattaforme informatiche?
Le LLGG n. 469/2021 disciplinano la figura del custode dell'identità quale ulteriore garanzia per la tutela della riservatezza del segnalante. Tuttavia, la legge non impone alle amministrazioni o agli enti di dotarsi di tale figura. Pertanto, non si considera, "obbligatoria" l'istituzione della figura del "custode".

Parole chiave: custode dell'identità-non obbligatorietà
Fonti normativa: Delibera 469 del 9.06.2021 recante linee guida in materia di whistleblowing

1.3. Ci sono indicazioni sui profili professionali più adeguati per rivestire il ruolo di custode dell'identità?
Le LLGG n. 469/2021 prevedono che il custode dell'identità possa coincidere con il RPCT, ma, laddove l'amministrazione o l'ente scelga di attribuire tale funzione ad un soggetto diverso dal RPCT, tale scelta dovrà ricadere su un soggetto che abbia gli stessi requisiti di terzietà ed imparzialità che la legge impone per nominare il RPCT. Fermi questi requisiti, la scelta è rimessa alla valutazione dell'amministrazione.

Parole chiave: custode dell'identità -requisiti- terzietà e imparzialità- valutazione dell'amministrazione
Fonti normativa: § 1 della Parte II della Delibera 469 del 9.06.2021 recante Linee guida in materia whistleblowing

1.4. Il custode dell'identità deve essere autorizzato al trattamento dei dati personali?
Si. Sul punto, le LLGG n. 469/2021 chiariscono che tutti i soggetti che trattano i dati – RPCT, componenti dell'eventuale gruppo di lavoro, custode dell'identità e personale degli altri uffici eventualmente coinvolti nella gestione della segnalazione di *whistleblowing* - devono comunque essere autorizzati e debitamente istruiti in merito al trattamento dei dati personali (ai sensi dell'art. 4, par. 10, 29, 32, §. 4 del Regolamento UE 2016/679 e art. 2-quaterdecies del d.lgs. 196 del 2003). Ciò in quanto nella documentazione trasmessa potrebbero essere presenti dati personali di altri interessati (es. soggetto cui sono imputabili le possibili condotte illecite).

Parole chiave: custode dell'identità -trattamento dati personali- autorizzazione
Fonti normativa: § 1 della Parte II della Delibera 469 del 9.06.2021 recante *Linee guida in materia di whistleblowing - Regolamento UE 2016/679 sulla protezione dei dati -art. 2-quaterdecies del d.lgs. 196 del 2003 recante il "Codice in materia di protezione dei dati personali"*

1.5. Il segnalante ha la possibilità di rivelare al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) la propria identità?
Le LLGG n. 469/2021 precisano che il RPCT è il soggetto legittimato, per legge, a trattare i dati personali del segnalante e, eventualmente, a conoscerne l'identità. Pertanto ove il segnalante lo ritenga opportuno, può svelare la propria identità al RPCT.

Parole chiave: segnalante – rivelazione identità –RPCT
Fonte: § 1 Parte I della Delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia whistleblowing

1.6. Quali sono le motivazioni che possono essere richieste dal Responsabile della prevenzione della corruzione e della trasparenza (RPCT) al custode dell'identità affinché venga sbloccata l'identità del segnalante?
Le LLGG n. 469/2021 chiariscono che si può consentire l'accesso del RPCT all'identità del segnalante esclusivamente dietro espresso consenso del custode dell'identità. E' opportuno che le amministrazioni disciplinino, nel PTPCT, o nell'atto organizzativo cui rinvia il Piano con cui si definisce la procedura, anche i casi e le motivazioni in presenza delle quali il custode dell'identità è autorizzato a disvelare i dati identificativi del segnalante al RPCT (si pensi a titolo esemplificativo, ai seguenti casi : (i) Il RPCT necessita di fornire i dati identificativi del *whistleblower* all'Autorità giudiziaria cui è stata trasmessa la segnalazione; (ii) il RPCT deve svolgere un'istruttoria complessa che richiede il coinvolgimento di più uffici interni e, quindi, per evitare di mettere a rischio il segnalante necessita di conoscerne l'identità (iii) il RPCT ha dubbi in merito alla qualifica di dipendente pubblico dichiarata dal segnalante)

Parole chiave: custode dell'identità – sblocco- identità del segnalante – richiesta del RPCT-motivazioni
Fonti normativa: § 2.1 e 22. Parte II della *Delibera 469 del 9.06.2021 recante Linee guida in materia di whistleblowing.*

1.7. Laddove il Responsabile della prevenzione della corruzione e della trasparenza (RPCT) coincida con il custode dell'identità, quale soggetto è competente a richiedere lo sblocco dei dati identificativi del segnalante?
Laddove il ruolo di RPCT coincida con quello del custode dell'identità sarà il Responsabile l'unico soggetto competente a sbloccare i dati identificativi del segnalante. In tale ipotesi, il sistema dovrà registrare l'accesso all'identità da parte del RPCT e, per evitare abusi da parte di quest'ultimo, sarebbe opportuno se non doveroso che il RPCT mantenga traccia delle ragioni che hanno reso necessario conoscere l'identità del segnalante.

Parole chiave: coincidenza- custode dell'identità – RPCT- sblocco - dati identificativi del segnalante-evidenza delle motivazioni
Fonti normativa: Delibera 469 del 9.06.2021 recante Linee guida in materia di whistleblowing

1.8 Nell'ipotesi in di avvicendamento di RPCT, il nuovo RPCT può accedere alle segnalazioni di whistleblowing ricevute dal RPCT precedente?
Le amministrazioni o gli enti possono disciplinare nel PTPCT, o nell'atto organizzativo cui il Piano rinvia, l'ipotesi di avvicendamento di RPCT. Secondo un principio di ragionevolezza e continuità dell'azione amministrativa è necessario che il nuovo RPCT abbia accesso alle segnalazioni ricevute anche dal RPCT precedente, specie se il procedimento sulla segnalazione non si sia ancora concluso. Il ruolo fondamentale nella gestione delle segnalazioni è infatti attribuito direttamente dalla legge al soggetto cui l'amministrazione conferisce l'incarico di RPCT.

Parole chiave: RPCT-avvicendamento– atto organizzativo-PTPCT-continuità -accesso alle segnalazioni di whistleblowing- RPCT nuovo- RPCT precedente
Fonte: delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing

1.9 Laddove l'amministrazione o l'ente decida di costituire un gruppo di lavoro a supporto del Responsabile della prevenzione della corruzione e della trasparenza (RPCT) l'accesso alla segnalazione di *whistleblowing* e ai dati ivi contenuti è consentito solo ai componenti del gruppo previamente individuati nel PTPCT o nell'apposito atto organizzativo cui il Piano rinvia?

Si, le LGG n. 469/2021 prevedono che l'accesso alle informazioni e ai dati contenuti nella segnalazione, è consentito solo a soggetti del gruppo preventivamente individuati dall'amministrazione o dall'ente nel PTPCT o nell'atto organizzativo cui il Piano rinvia. Si raccomanda, inoltre, che il modello organizzativo adottato definisca le responsabilità in tutte le fasi del processo di gestione delle segnalazioni, con particolare riguardo agli aspetti di sicurezza e di trattamento delle informazioni. Tali misure trovano specifica applicazione in relazione alle caratteristiche del sistema informatico realizzato e si inseriscono nell'ambito dei presidi di sicurezza delle informazioni di carattere tecnico ed organizzativo predisposti dall'amministrazione nella gestione dei sistemi informativi.

Parole chiave: accesso- segnalazione di whistleblowing -componenti gruppo lavoro-identificati- atto organizzativo-PTPCT

Fonte: § 2.2. Parte II della delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing

1.10 I componenti del gruppo di lavoro individuati dall'amministrazione/ente nel PTPCT o nell'atto organizzativo possono richiedere al custode l'identità del segnalante?

Le LLGG n. 469/2021 chiariscono che custode delle identità, dietro esplicita e motivata richiesta, può consentire al RPCT di accedere all'identità del segnalante.

In merito a tali profili, al fine di fornire indicazioni utili, si descrive a titolo esemplificativo la prassi utilizzata da Anac. La piattaforma distingue il ruolo del Coordinatore (dirigente dell'UWHIB) e degli istruttori (funzionari dell'UWHIB). Il Coordinatore riceve le segnalazioni di *whistleblowing* e le assegna a ciascun funzionario chiamato a gestire concretamente le singole segnalazioni. Nel caso in cui sia necessario conoscere l'identità del segnalante (ad esempio nel caso di trasmissione dati identificativi alle Procure), il Coordinatore (e non l'istruttore) formula la richiesta di autorizzazione al Custode dell'Identità.

Parole chiave: componenti gruppo lavoro - identità del segnalante -custode dell'identità –segnalazioni di whstleblowing- prassi ANAC
Fonte: § 2.2. parte II della delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing

1.11 E' configurabile una responsabilità in capo ai componenti del gruppo di lavoro?
Le LLGG n. 469/2021 chiariscono che, al fine di rafforzare le misure a tutela della riservatezza del segnalante, è opportuno che le amministrazioni introducano nei codici di comportamento, adottati ai sensi dell'art. 54, co. 5, del d.lgs. 165/2001, 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, con i dati e le informazioni in essa contenuti. La violazione dei doveri contenuti nel codice di comportamento è fonte di responsabilità disciplinare.

Parole chiave: componenti gruppo di lavoro- codice di comportamento- violazione doveri di comportamento- responsabilità disciplinare
Fonte: § 3.1. della Parte I e § 1 della Parte II della delibera ANAC 469 del 9 giugno 2021 recante *Linee guida in materia di whistleblowing*

1.12. I componenti del gruppo di lavoro possono accedere alla Piattaforma informatica di gestione delle segnalazioni di whistleblowing in modo autonomo dal Responsabile della prevenzione della corruzione e della trasparenza (RPCT)?
Il RPCT riceve le segnalazioni di *whistleblowing* e provvede ad assegnarle nella Piattaforma informatica ai singoli componenti del gruppo di lavoro per coadiuvarlo nello svolgimento dell'attività istruttoria. 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.

Parole chiave: gestione delle segnalazioni di whistleblowing - componenti gruppo di lavoro–accesso autonomo Piattaforma informatica
Fonte: delibera ANAC 469 del 9 giugno 2021 recante *Linee guida in materia di whistleblowing*

1.13. Il Responsabile della prevenzione della corruzione e della trasparenza (RPCT) assegna, di volta in volta, la segnalazione di *whistleblowing* ai componenti del gruppo di lavoro individuati dall'amministrazione?
Nelle LLGG n. 469/2021 è chiarito che Il RPCT è il soggetto legittimato per legge a ricevere e prendere in carico le segnalazioni di *whistleblowing* e quindi a trattare i dati personali del segnalante e, eventualmente, a conoscerne l'identità.
Ne consegue che l'assegnazione di una segnalazione di *whistleblowing* deve essere, di volta in volta, disposta dal RPCT.

Parole chiave: assegnazione del RPCT- segnalazione di whistleblowing - componenti gruppo lavoro
Fonte: cfr. *§ 1 Parte II della delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing - Legge 30 novembre 2017, n. 179 – art. 54bis del decreto legislativo 30 marzo 2001, n. 165*

1.14. Il soggetto cui è stata assegnata una segnalazione di whistleblowing può riassegnarla a sua volta ad un collega/ufficio ritenuto più appropriato?

No, la facoltà di assegnazione delle segnalazioni di *whistleblowing* è consentita al solo RPCT.

Parole chiave: riassegnazione – soggetto competente – segnalazioni di whistleblowing
Fonte: delibera ANAC 469 del 9 giugno 2021 recante *Linee guida in materia whistleblowing*

1.15. L'assegnazione di una segnalazione di whistleblowing è revocabile?
L'assegnazione di una segnalazione di *whistleblowing* può essere revocata dal RPCT con apposita motivazione.

Parole chiave: assegnazione- segnalazioni di whistleblowing - revoca -motivazione
Fonte: delibera ANAC 469 del 9 giugno 2021 recante *Linee guida in materia di whistleblowing*

1.16 Quale è il termine di conservazione delle segnalazioni di whistleblowing?

Nelle LLGG n. 469/2021, con riferimento ai termini della conservazione delle segnalazioni, che sono stati valutati con il Garante per la protezione dei dati personali, si è precisato che i dati raccolti vadano conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
Le LLGG n. 469/2021 non prevedono, quindi, un termine di conservazione delle segnalazioni che sia vincolante per tutte le amministrazioni. Spetta, infatti, a ciascuna di esse, in base alle esigenze specifiche, definire nel PTPCT o nell'atto organizzativo cui il Piano rinvia, modalità e termini di conservazione dei dati, appropriati e proporzionati ai fini della procedura di *whistleblowing*.
Per le segnalazioni ricevute da ANAC, alla luce delle specifiche esigenze e competenze dell'Autorità, è stato previsto un termine minimo di conservazione delle segnalazioni, pari almeno a 10 anni. Nel caso in cui sia instaurato un giudizio, tale termine si prolunga fino alla conclusione del giudizio stesso.
Parole chiave: conservazione della segnalazione di whistleblowing –termini conservazione ANAC-giudizio
Fonti normativa: § 2 della Parte II della Delibera 469 del 9.06.2021 recante Linee guida in materia di whistleblowing)

1.17. Il termine di conservazione delle segnalazioni di whistleblowing deve essere fissato per tutte le segnalazioni, qualsiasi sia il canale utilizzato dal segnalante?
Si, l'esigenza di prevedere un termine di conservazione dei dati vale per tutte le segnalazioni di *whistleblowing* ricevute dal RPCT, qualunque sia il canale utilizzato. Non vi sono, infatti, elementi per prevedere una differenziazione di trattamento.

Parole chiave: segnalazioni di whistleblowing- termine di conservazione – qualsiasi canale di segnalazione
Fonti normativa: Delibera 469 del 9.06.2021 recante Linee guida in materia di whistleblowing

1.18. Con quale modalità l'amministrazione o l'ente deve rendere pubblico il sistema informatico di gestione delle segnalazioni di *whistleblowing*?
le LGG n 469/2021 chiariscono che l'Amministrazione dà notizia dell'adozione del sistema applicativo informatico di gestione delle segnalazioni di *whistleblowing* nella *home page* del proprio sito istituzionale in modo chiaro e visibile. E' rimessa alla valutazione dell'amministrazione se rendere tale informativa come una news o come un contenuto permanente.

Parole chiave : pubblicazione –sito web- modalità - notizia – sistema informatico- gestione segnalazioni di whistleblowing
Fonte normativa: delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing

1.19 L'indirizzo web della piattaforma deve essere pubblicato sul sito istituzionale dell'amministrazione?
Le LLGG n. 469/2021 precisano che l'indirizzo web della piattaforma è raggiungibile da Internet, ma l'amministrazione/ente può decidere di non renderlo pubblico sul sito istituzionale. Ciò in quanto la pubblicazione del link alla piattaforma sul sito internet dell'Ente può esporre alla possibilità che il sistema venga utilizzato impropriamente da qualunque utente (ad esempio soggetti non dipendenti dell'Ente né delle imprese fornitrici) per inviare segnalazioni che non rientrano tra i casi di *whistleblowing* previsti dalla normativa. L'afflusso di segnalazioni non pertinenti potrebbe non consentire un uso proprio della piattaforma dedicata, tenuto conto che spetta in primo luogo al RPCT, per ogni segnalazione, la valutazione sulla sussistenza dei requisiti essenziali contenuti nel co. 1 dell'art. 54-bis del d.lgs. 165/2001 per poter accordare o meno al segnalante le tutele ivi previste.

Pertanto, l'amministrazione, se lo ritiene opportuno, può decidere di adottare altre forme di pubblicità per i dipendenti e i collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica (ad es. mediante comunicazione diretta del link al momento della sottoscrizione del contratto di fornitura).
La previsione delle LLGG è quindi intesa a salvaguardare il buon funzionamento della piattaforma dedicata e di conseguenza la tutela del *whistleblower.*

Parole chiave: pubblicazione -indirizzo web piattaforma- link piattaforma -forme di pubblicità– dipendenti – collaboratori- imprese fornitrici beni- imprese fornitrici servizi- imprese che realizzano opere-uso improprio link piattaforma
Fonte normativa: § 1 e 2.2. Parte II della delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing

1.20 Esistono requisiti specifici che la Piattaforma informatica di gestione delle segnalazioni di *whistleblowing* deve prevedere per evitare che il segnalante fornisca dati identificativi falsi o non corretti (es. Mario o Maria Rossi)?

Non vi sono requisiti specifici che la Piattaforma informatica deve prevedere per evitare il problema sollevato. Le contromisure al problema sono infatti strettamente correlate al livello tecnico dei sistemi dell'Ente.

Parole chiave : requisiti Piattaforma–rischio-dati identificativi falsi o non corretti- segnalante
Fonte normativa: Delibera 469 del 9.06.2021 recante Linee guida in materia di whistleblowing

1.21 l'Amministrazione, nei casi in cui l'accesso alla piattaforma informatica è mediato da dispositivi firewall o proxy, come può garantire la non tracciabilità del segnalante?

Le LLGG n. 469/2021 chiariscono che la procedura di gestione delle segnalazioni di *whistleblowing* utilizzata deve tutelare la riservatezza dell'identità del segnalante, del contenuto della segnalazione, della documentazione ad essa allegata nonché dell'identità di eventuali soggetti segnalati, garantendo l'accesso a tali informazioni solo ai soggetti autorizzati e previsti nell'iter procedurale. 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. La tecnologia TOR rappresenta una delle possibili soluzioni per l'anonimizzazione dei dati del segnalante

Parole chiave: tutela riservatezza- identità del segnalante- non tracciabilità- piattaforma informatica- firewall- proxy- dati di navigazione -strumenti di anonimizzazione –-tecnologia TOR
Fonte normative: § 2.2. Parte II della delibera ANAC 469 del 9 giugno 2021 recante Linee guida in materia di whistleblowing

1.22. La piattaforma deve registrare gli accessi dei diversi utenti?

Si. Le LLGG n. 469/2021 chiariscono che occorre tracciare l'attività degli utenti del sistema nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione di *whistleblowing*. I relativi log devono essere adeguatamente protetti da accessi non autorizzati e devono essere conservati per un termine congruo rispetto alle finalità di tracciamento. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante. Il tracciamento può essere effettuato esclusivamente al fine di garantire la correttezza e la sicurezza del trattamento dei dati.
In ogni caso, La disciplina della gestione degli accessi e dei log applicativi rientra nella serie di atti organizzativi che l'amministrazione deve adottare per adempiere alle previsioni in materia di sicurezza informatica e protezione dei dati personali.

Parole chiave: Tracciamento degli accessi – utente – log
Fonte normative: § 2.2. Parte II della delibera ANAC 469 del 9 giugno 2021 recante "Linee guida in materia di whistleblowing)"